Tabla de anexos

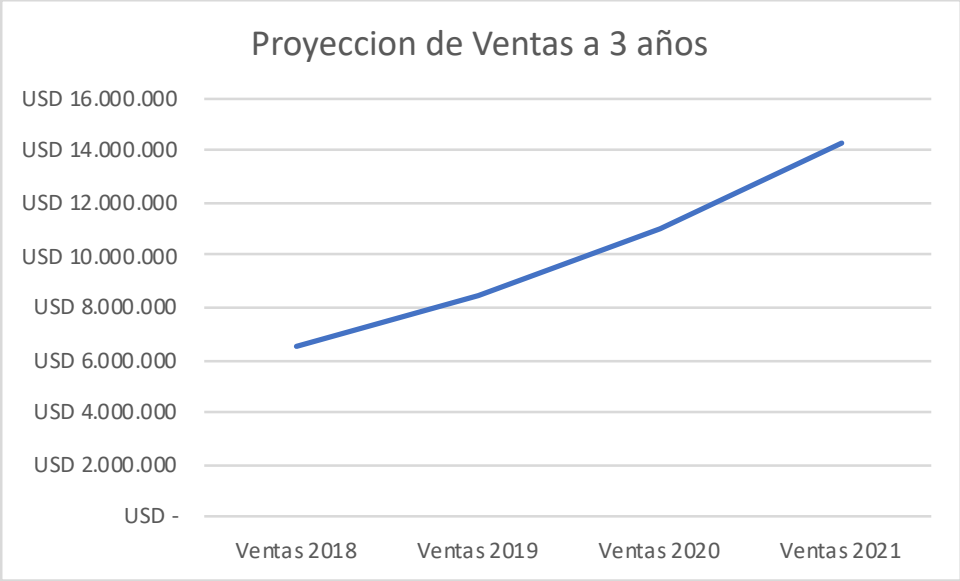
Anexos

Anexo 1 Informe comercial “Empresa SI” 2018

Pais	Area	Monto USD	
Chile	Total x Pais	USD	34.479.362
Chile	Seguridad Corporativa	USD	24.084.720
Chile	Consultoria	USD	1.643.702
Chile	Canal Electronico	USD	5.095.964
Chile	SGS	USD	3.654.976
Argentina	Total x Pais	USD	20.472.608
Argentina	Seguridad Corporativa	USD	12.234.271
Argentina	Consultoria	USD	2.636.291
Argentina	Canal Electronico	USD	3.053.701
Argentina	SGS	USD	2.548.345
Perú	Total x Pais	USD	10.873.648
Perú	Seguridad Corporativa	USD	8.802.205
Perú	Consultoria	USD	1.464.552
Perú	Canal Electronico	USD	330.836
Perú	SGS	USD	276.056
Colombia	Total x Pais	USD	6.747.530
Colombia	Seguridad Corporativa	USD	4.917.355
Colombia	Consultoria	USD	359.952
Colombia	Canal Electronico	USD	719.767
Colombia	SGS	USD	750.456
Total general		USD	72.573.148

% Participacion Consultoria 2018		
Total Ventas Consultoria	USD	6.104.497
Chile		26,93%
Argentina		43,19%
Peru		23,99%
Colombia		5,90%

% Participacion Consultoria 2018 VS Otras	
Seguridad Corporativa	72,88%
Consultoria	5,33%
Canal Electronico	10,67%
SGS	11,12%



Anexo 2 Líneas de negocio "Empresa SI" Colombia

Las 4 líneas de negocio de la "Empresa SI" son:

- Servicios gestionados de seguridad – CDC (Centro de Ciberdefensa)
- Consultoría
- Seguridad Corporativa
- Seguridad en Canal Digital

1. **Seguridad corporativa**

Esta línea tiene como objetivo proporcionar soluciones a controles de seguridad basado en estándares de seguridad, tecnologías en seguridad de la información y ciberseguridad en el entorno IT (Tecnologías de la Información) y OT (Tecnologías de la Operación), sea en modalidad en sitio o Nube, a necesidades o problemas que posee un cliente en la operación y funcionamiento diario de una empresa, enfocándose a diversos niveles de protección y control como, por ejemplo:

- **Soluciones para la Protección del Perímetro de Negocios**

Estas se enfocan en las aplicaciones de negocio disponibles para que las organizaciones puedan prestar su servicio a sus clientes o logren relacionarse con sus proveedores o aliados en el negocio. Para brindar estas soluciones de protección, se cuenta con socios tecnológicos como F5, Arbor Networks, Waratek y HP Enterprise. Entre estas soluciones se destacan las siguientes:

  - Solución de protección de aplicaciones
  - Solución de protección de la disponibilidad
  - Autoprotección de aplicaciones

- Evaluación de código

- **Soluciones para el Control del Perímetro de Usuarios**

Conviene que las organizaciones puedan contar con al menos dos perímetros claramente separados y controlados, a saber: 1) el perímetro de usuarios y 2) el perímetro de negocios. En el primero ocurre principalmente el tráfico de los usuarios y de los sistemas internos hacia el exterior (navegación, correo electrónico, video, etc). Para brindar estas soluciones de protección, la empresa cuenta con socios tecnológicos como Palo Alto Networks, Symantec, McAfee, Tenable, CISCO y FireEye. Entre estas soluciones se destacan:

- Protección de acceso e intrusiones
- Protección de la navegación
- Gestión de vulnerabilidades
- Protección del correo
- Protección antimalware

- **Soluciones para el Control de la Actividad de Usuarios**

La red interna de una organización constituye un ambiente en el que se entregan amplios niveles de confianza a diversos usuarios. Uno de los problemas más relevantes es, por lo tanto, el abuso de esta confianza o, incluso, la traición a la misma. Esto se traduce, por ejemplo, en el incumplimiento de ciertas políticas, el fraude y el sabotaje, así como en otras amenazas serias a la seguridad de una compañía.

Este modelo representa las soluciones que controlan y analizan las actividades de los usuarios en la red interna del cliente. Esto, con el objetivo de conocer, por ejemplo, las actividades que están realizando los usuarios privilegiados y el comportamiento anómalo de estos, así como monitorear sistemas operativos, servidores y bases de datos. Para brindar estas soluciones de protección se cuenta con socios tecnológicos como IBM, Imperva, McAfee, Cyberark, SAT Control Suite, Vormetric Data Security y Securonix. Algunas de estas soluciones son:

- Solución de protección de bases de datos
- Solución de prevención de fuga de información
- Control de usuarios privilegiados
- Cifrado de datos
- Solución de análisis de comportamiento anómalo de usuarios

- **Soluciones para la Protección frente a amenazas avanzadas**

Los mayores ataques de la historia de la seguridad informática han ocurrido de manera más bien reciente. Los cibercriminales han utilizado estrategias avanzadas dirigidas y focalizadas en objetivos muy concretos. Esto, haciendo uso de un amplio conocimiento de los controles internos y de los mecanismos de evasión existentes en la actualidad.

Las amenazas existentes involucran distintos tipos de técnicas. Entre estas se encuentran la ingeniería social, el malware, el hacking y el robo de credenciales, entre otras, las cuales pueden ser ejecutadas en una organización durante años, de manera continua, sin ser detectadas. Para brindar estas soluciones de protección, la "*Empresa SI"* cuenta con socios tecnológicos como Crowdstrike, Securonix y FireEye. Entre las soluciones disponibles se destacan:

- Solución de protección del Endpoint

- Solución de análisis de comportamiento anómalo de usuarios
- Solución de Sandbox en la navegación y en el correo electrónico

2. Seguridad en Canal Digital

La visión de la "*Empresa SI*" de la seguridad en canales Electrónicos, basada en la experiencia obtenida en el trabajo junto a sus clientes, los ha llevado a la convicción que la mejor forma de mitigar el riesgo en la operación es mediante la implementación de múltiples controles y capas de seguridad que abarquen todo el quehacer de los Canales Electrónicos.

Considerando lo anterior y, dado que ninguna medida de seguridad es suficiente por sí sola, "*Empresa SI"* ha definido su exclusivo modelo multicapa de seguridad. Este se enfoca en canales electrónicos y se centra en las necesidades reales de sus clientes. Esto lo convierte en el único servicio diferenciador de la compañía. Para brindar estas soluciones de protección, se cuenta con socios tecnológicos como IBM, Entrust, Vasco, Nice Actimize y RSA. Entre las soluciones disponibles se encuentran:

- Protección del Endpoint
- Protección de la identidad
- Protección de la aplicación
- Protección de la transacción
- Protección de la operación
- Protección de los procesos internos

3. Servicios gestionados – SGS

Los Servicios Gestionados son ofrecidos desde el CDC (Cyber Defense Center) de "Empresa SI" sustentados por la certificación ISO 27001 y las diversas labores desarrolladas por el equipo de especialistas abocados a diversas tareas de monitoreo, investigación, operación y mejora continua; aplicando las mejores prácticas de la industria y minimizando los costos de operación de las organizaciones.

Estos servicios se ofrecen utilizando la plataforma de correlación SIEM, líder en la industria, herramientas de inteligencia de amenaza de última generación con el fin de anticiparse a ellas y portales de acceso a clientes para brindar visibilidad de la actividad maliciosa detectada y tendencias, permitiendo al cliente una mejor toma de decisiones.

En esta línea se ofrecen las siguientes 3 soluciones:

- **RiskMonitor**: ofrece la protección de la información de la empresa, a través de diversos procesos y tecnologías de seguridad informática. Las soluciones que permite brindar son:
    - Detección
    - Personalización
    - Respuesta a incidentes
    - Portales para visibilidad
- **RiskManagement*:*** ofrece la administrar el riesgo haciéndose cargo de las plataformas. Esto, con el fin de minimizar los costos operativos asociados y las necesidades de la

empresa de entrenar personal en materia de tecnologías fuera del core del negocio. Las soluciones disponibles son:

  - Administración de las plataformas de seguridad
  - Monitoreo de disponibilidad y salud de dispositivos
  - Soporte

- **RiskControl** es el servicio gestionado completo. Este monitorea, administra y soporta las plataformas de seguridad del cliente, entregando un nivel de protección y respuesta verdaderamente superior. Lo anterior:
  - Permite agilizar el proceso de respuesta ante un incidente ya que es posible tomar medidas de mitigación directamente en las plataformas y no derivar a otros las acciones necesarias.
  - Permite hacer un análisis de mayor profundidad y con mayor rapidez de las amenazas existentes. Esto, al contar con la información inmediata directamente de las plataformas.
  - Facilita que los equipos expertos de monitoreo y administración están permanentemente comunicados, lo que permite un mejor conocimiento y toma de decisiones con respecto a la protección y la mitigación.

2. Consultoría

La consultoría de la "*Empresa SI"* a nivel corporativo tiene como fin ser un aliado del área de tecnología para así apoyar la estrategia de negocio de las compañías.

Durante los ocho años de presencia en el mercado colombiano se han ofrecido múltiples servicios de consultoría, los cuales gravitan alrededor de cinco temáticas básicas. Estas son:

1. Estándares y normativas:

Se enfoca en realizar una evaluación de la situación de seguridad de la organización, considerando estándares y normativas de seguridad regulatorios o de la industria, corporativos o locales y nacionales o internacionales. Esto, con el fin de apoyar la adopción y el cumplimiento de esos estándares y normativas. Entre otros, se consideran los siguientes aspectos:

- Normativas del gobierno para Instituciones del Estado.
- Leyes de protección de datos personales y otras específicas como la protección de datos médicos.
- PCI-DSS. Estándar de Seguridad de datos de la Industria de tarjetas de crédito.
- SOX-404. Controles y procedimientos internos para empresas que transan acciones de forma pública en el mercado de USA.
- SWIFT. Programa de seguridad de clientes (para transferencia internacional de fondos bancarios).

2. Buenas prácticas:

En este aspecto se busca acompañar a las empresas y apoyarlas en la implementación efectiva de controles de seguridad que conduzcan a la definición, formalización, protección, monitoreo y respuesta ante situaciones que amenacen la seguridad de la información. Entre otros, se consideran aquí los siguientes aspectos:

- Casos de uso o reglas de negocio u operacionales para soluciones de seguridad.
- Clasificación de información.
- Concientización de seguridad (awareness).
- Formación de equipos de respuesta ante incidentes.
- Políticas y procedimientos de seguridad informática y de seguridad de la información.
- Evaluación de seguridad de data center.

3. *Continuidad de negocio:*

Este servicio tiene como objetivo preparar a la empresa para responder y recuperarse de situaciones que pueden poner en peligro la continuidad de las actividades críticas de la organización. Se consideran aquí los siguientes puntos:

- Construcción y actualización de planes.

1. Planes de continuidad de negocios (BCP - Business Continuity Plan).
2. Planes de recuperación de desastres Information technology - IT (DRP - Disaster Recovery Plan).

- Diagnóstico y auditorías de cumplimiento.

3. Planes BCP-DRP.
4. Sistema de gestión de continuidad de negocio (SGCN) según ISO 22301.
5. Procesos de análisis de impactos en el negocio (BIA - Business Impact Analysis) según ISO 22317.

- Especificación e implantación de SGCN según ISO 22301.

- Preparación y desarrollo de actividades específicas en gestión de continuidad del negocio.

6. Desarrollo de políticas, normativas y guías metodológicas para los procesos de gestión y de preparación de planes de continuidad.
7. Realización o revisión de análisis de impactos en el negocio (BIA) y evaluación de riesgos (RIA – Regulatory Impact Analysis).
8. Estudio de situación de estrategias de continuidad y preparación de carteras de proyectos asociados.
9. Construcción de planes de recuperación y seguimiento en la implementación de proyectos tecnológicos para DRP.
10. Preparación y acompañamiento en la ejecución de pruebas de planes de continuidad.

4. Gestión del riesgo y la seguridad:

Este servicio busca ayudar a la organización en la identificación, la evaluación y la gestión de los riesgos que enfrentan sus procesos y activos de información. Como su nombre lo indica, este cubre dos componentes básicos:

- Sistema de gestión de la seguridad.
- Gestión de riesgo.

5. Entorno tecnológico:

Este servicio se enfoca en evaluar y orientar la reducción o mitigación de los riesgos de seguridad en las plataformas tecnológicas y en los procesos relacionados con su administración.

Como es natural, si estos aspectos se ven afectados, pueden llegar a perjudicar el *core* del negocio.

Entre los aspectos atendidos acerca de este tema se encuentran los siguientes:

- Evaluación de la arquitectura de red.
- Evaluación de vulnerabilidades.
- Evaluación de la configuración de dispositivos de seguridad.
- *Ethical hacking*.
- Análisis de *logs*.
- Evaluación de seguridad de aplicaciones.
- Evaluación de seguridad de redes industriales.

Anexo 3 Línea de negocio de consultoría en Argentina

La línea de negocio de consultoría en la sucursal de Argentina, se toma como base de comparación por su madurez interna en ventas en 2018 con un 43,19% de la participación en ventas de esta línea de la "*Empresa SI"* a nivel corporativo y está dividida en dos servicios: servicios consultivos y evaluaciones tecnológicas.

Servicios consultivos: Están divididos en 5 temáticas:

1. Evaluación
    - Evaluaciones de seguridad: dirigidas a identificar lo que necesita una compañía para cumplir con las normativas y estándares como: ISO/IEC 27001 e ISO/IEC 27002, PCI-DSS, BCRA A4609, Data centers, COBIT
    - Evaluaciones tecnológicas: dirigida a evaluar el estado de seguridad en diferentes áreas como: seguridad de redes, seguridad de FWs, seguridad de plataformas, seguridad de bases de datos, seguridad de aplicaciones, seguridad en AD y arquitecturas de red.
    - Riesgo de TI y Riesgo de Seguridad de Información (SI)

2. Protección:
    - Equipos de respuesta a incidentes
    - Continuidad tecnológica
    - Continuidad de negocios

3. Buenas prácticas:
    - Desarrollo de políticas y procedimientos
    - Campañas de concientización
    - Clasificación de activos de información
    - Desarrollo de baselines
    - Seguridad en proyectos de seguridad

4. Cumplimiento:
    - De estándares y normativas como SOX e ISO 27001
    - Normativas locales como protección de datos personales (LPDP y GDPR) y comunicaciones Banco Central
    - Observaciones de Auditorías

5. Gestión:
    - Planes estratégicos
    - Planes de seguridad
    - Sistema de gestión de seguridad de la información
    - Sistema de gestión de continuidad de negocios
    - Sistema de gestión de riesgo
    - Sistema de gestión de Ciberseguridad

Servicios de evaluaciones tecnológicas: están divididos en 6 temáticas:

1. Evaluación de arquitectura: Verifica la correcta estructuración de la red de comunicaciones desde la perspectiva de: Protección del perímetro, segmentación, control de accesos, monitoreo y detección e incorporación de soluciones de seguridad.
2. Evaluación de vulnerabilidades: Revisa la seguridad de diferentes ámbitos de TI en busca de las debilidades o vulnerabilidades técnicas presentes.
3. Ethical Hacking: Prueba las vulnerabilidades existentes para comprobar si es posible explotarlas para acceder a los activos de la empresa de forma no autorizada.
4. Evaluación de configuración de dispositivos de seguridad: Se enfocan en comprobar que los dispositivos de seguridad como Firewalls e IPS, estén utilizados adecuadamente y cumplan el propósito de protección que se espera de ellos.
5. Revisión de seguridad de servicios: Revisa la seguridad de servicios claves en la organización como Directorios activos (A.D.), Correo Electrónico y Domain Name Systems (DNS). Busca debilidades en la configuración de las condiciones de seguridad.
6. Análisis de tráfico: Revisa el tráfico hacia Internet en busca de indicios de tráfico malicioso y del uso de aplicaciones peligrosas para la protección de la información.

En los últimos años han desarrollado nuevos servicios al identificar nuevas necesidades del mercado y de acuerdo a los incidentes de seguridad de la información que se han presentado como:

- Servicios de Ciberseguridad sobre Sistemas Industriales (IACS): aplican para cada fase del ciclo de vida de seguridad en los procesos de automatización. La metodología de evaluación de riesgo exclusiva para la Ciberseguridad Industrial e Infraestructuras Críticas que llamamos Cyber-PHA. Ofrece diferentes tipos de assessments que se pueden realizar sobre los sistemas industriales:
    - GAP Analisys: son evaluaciones que se desarrollan principalmente en entrevistas para conocer las prácticas actuales de la planta y compararlas contra mejores prácticas.
    - Pasive Analisys: se desarrollan asistidos con herramientas para levantar datos, informaciones de las redes y sistemas industriales.
    - Active Non Intrusive: se realizan asistidos con herramientas homologadas y certificadas con capacidad de dialogar con los sistemas industriales
    - Active Intrusive: se realizan con herramientas que pueden provocar una interrupción o efecto indeseado en los sistemas industriales.
    - Destructivas: se realizan con la finalidad de detectar vulnerabilidades por medio de su explotación.

- Servicios de Assessment entornos Cloud: enfocados a los diferentes ataques que se realizan hacia los usuarios, la tecnología y los procesos como:
    - Secuestro de servicios utilizando técnicas de ingeniería social.
    - Secuestro de sesión utilizando ataques de XSS.
    - Ataques DNS.
    - SQL injection.

- Wrapping Attack.
- Secuestro de servicio utilizando sniffing de red.
- Secuestro de sesión mediante Session Riding.
- Side Channel Attack o Cross-guest VM.
- Ataques de criptoanálisis.
- DoS y DDoS.

Estos servicios de consultoría cuentan con las siguientes tecnologías como soporte: GlobalSuite, Tenable, Smartfense, Fortify, Paloalto, Symantec, Firemon e IBM.

Anexo 4 Clientes actuales “Empresa SI” Colombia

Financiero

- ATH
- ACH
- BANCO DE LA REPUBLICA
- BANCO POPULAR
- BANCO AVVILLAS
- BANCO DE OCCIDENTE
- BANCO DE BOGOTA
- BANCO WWB (CALI)
- CFA (MDE)
- CONFIAR (MDE)
- COLPATRIA
- DAVIVIENDA
- BANCO ITAU
- REDEBAN
- COTRAFA (MDE)
- BANCOLOMBIA
- BANCO FALABELLA
- CREDICORP CAPITAL

Retail

- CENCOSUD
- HOMECENTER
- CORONA

Seguros

- SEGUROS BOLIVAR
- FOGAFIN

Comunicaciones

- CLARO
- ECOM SAS
- MATRIXTECH (MDE)

Energia

- VATIA (CLO)

Salud

- FUNDACION SANTAFE
- IPS MEDELLIN

Transporte

- RUNT

Construcción

- CONSTRUCTORA BOLIVAR
- EXTRUSIONES (MDE)
- PISA (Cali)

Gobierno

- MINISTERIO DE DEFENSA
- SECRETARIA DE MOVILIDAD
- COLDEPORTES
- INVIMA
- UPME
- ALCALDIA DE ENVIGADO
- DIPOL
- FISCALIA

Servicios

- COMFAMA
- MERCADO LIBRE
- DESPEGAR

Agricultura

- MOLINOS ROA

Anexo 5 Cuestionario visita diagnostico

En la visita de diagnóstico se realizarán las siguientes preguntas que guiarán el proceso de conocimiento de las necesidades del cliente:

1. ¿Cuántas personas tiene actualmente la empresa?
2. ¿Cuántos de esas personas tienen dispositivos que poseen acceso de red a Internet?
3. ¿Cuántas personas conforman su equipo de seguridad de la información o ciberseguridad?
4. ¿El área de seguridad a quien le reporta?
5. ¿Qué tipo de normativa local o internacional tiene que cumplir la compañía, adicional a (nombrar las que se investigaron)?
6. ¿Cuál es su dolor o necesidad actual como compañía en seguridad de la información y ciberseguridad?
7. ¿Realizan pruebas de seguridad en sus redes? ¿Qué tipo de pruebas realizan y cada cuánto?
8. ¿Cuál es la estructura organizacional?
9. ¿Quién es el perfil del decisor o que toma decisiones de compra de la compañía para los proyectos en seguridad de la información y ciberseguridad?
10. ¿Qué tipo de proyectos tiene actualmente la compañía en Seguridad de la Información y ciberseguridad?
11. ¿Ha contratado anteriormente servicios de consultoría? ¿Cuales?
12. ¿Ha tenido algún incidente de seguridad en el cual pueda ser de ayuda? Descríbame lo sucedido y en qué estado se encuentra

13. ¿Posee presupuesto independiente para contratación de servicios consultivos en seguridad de la información o ciberseguridad?

Anexo 6 Glosario

El Glosario utilizado está basado en el glosario de la terminología ISO27000 *(iso27000.es, 2012)* y fue actualizado con nuevos conceptos utilizados en este documento;

- **A**

ABM

(inglés: Assesment Business Management). Administración de la seguridad de la información en una Compañía (Cardos, 2011)

Acción correctiva

(inglés: Corrective action). Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Acción preventiva

(inglés: Preventive action). Medida de tipo proactivo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.

Activo

(inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Active Directory (AD)

Véase: Directorio Activo

Amenaza

(inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Auditor

(inglés: Auditor). Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.

Auditoría

(inglés: Audit). Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

Autenticación

(inglés: Authentication). Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad

(inglés: Authenticity). Propiedad de que una entidad es lo que afirma ser.

- **B**

Baseline

Véase: Línea Base.

BCRA A4609

Normativa en Argentina emitida por el Banco Central de la República Argentina para las entidades Financieras y cámaras electrónicas de compensación. Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información. Con un punto en control y monitoreo de seguridad informática.

Business Continuity Plan

Véase: Plan de continuidad del negocio.

- **C**

Centro de Datos

(inglés: Data Center). Sitio donde se albergan servidores, equipos de comunicación y seguridad de una o más compañías, de gran infraestructura donde se acondiciona con fuentes de alimentación, ventilación, temperatura y seguridad física e informática necesaria para tener estos activos funcionando todo el tiempo con mínimos de interrupción en disponibilidad.

CISA

Certified Information Systems Auditor. Es una acreditación ofrecida por ISACA.

CISM

Certified Information Security Manager. Es una acreditación ofrecida por ISACA.

CISSP

Certified Information Systems Security Professional. Es una acreditación ofrecida por ISC2.

Circular 007 de 2018 de la SFC

Circular emitida por la Superintendencia de Colombia para las entidades financieras, con el fin de complementar los requerimientos mínimos para la gestión del riesgo de ciberseguridad en las entidades vigiladas y estándares de seguridad para las pasarelas de pago con el fin de fortalecer la protección de la información de los consumidores financieros. (007, 2018)

Circular externa 005 de 2019 de la SFC

Imparte instrucciones relacionadas con el uso de servicios de computación en la nube. (005, 2019)

Checklist

Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

CobiT

Control Objectives for Information and related Technology. Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacional y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Confidencialidad

(inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Costos Fijos

Los costos fijos son aquellos que no varían en función de los productos ofrecidos y servicios prestados.

Costos Variables

Los costos variables son aquellos que varían en función de los productos ofrecidos y servicios prestados.

- **D**

Data Center

Véase: Centro de Datos.

Declaración de aplicabilidad

(Ingles: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Desastre

(inglés: Disaster). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva o directriz

(inglés: Guideline). Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Directorio Activo

Es el acrónimo para referirse a un directorio de usuarios de una empresa que están cobijados por una administración global, y donde los usuarios realizan sus procesos de

autenticación. Este nombre hace referencia a la funcionalidad de LDAP de la marca Microsoft.

Disponibilidad

(inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

DNS

(Ingles: Domain Name System). Sistema que resuelve un nombre de dominio a una dirección de IP, protocolo que es utilizado para las comunicaciones en Internet para conectarse a un servidor.

- **E**

Economías de Campo

Este término se refiere a las ventajas que existen en términos de costos cuando una empresa utiliza los mismos recursos para distintos procesos.

Evaluación de riesgos

(inglés: Risk assessment). Proceso global de identificación, análisis y estimación de riesgos.

- **F**

Firewall

Control de seguridad perimetral que permite o deniega los accesos de peticiones de comunicación a la empresa o desde la empresa hacia Internet o segmentos de red de la organización. Buscando no permitir acceso o peticiones no permitidas por la organización.

FWs

Véase: Firewall. La “s” significa la palabra en plural

- **G**

Gestión de incidentes de seguridad de la información

(Ingles: Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos

(inglés: Risk management). Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

GDPR

General Data Protection Regulation. Reglamento general de protección de datos propuesto por la Unión Europea. (Wachter, 2018)

- **H**

HIPAA

Acrónimo en Ingles Health Insurance Portability and Accountability Act, que hace referencia a la Ley de Transferencia y Responsabilidad de Seguro Médico de 1996 para proteger la información medica (Cáncer, 2016)

- **I**

Identificación de riesgos

(inglés: Risk identification). Proceso de encontrar, reconocer y describir riesgos.

Impacto

(inglés: Impact). El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.

Incidente de seguridad de la información

(inglés: Information security incident). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad

(inglés: Integrity). Propiedad de la información relativa a su exactitud y completitud.

ISACA

Information Systems Audit and Control Association. Publica CobiT y gestiona diversas acreditaciones personales en el ámbito de la auditoría de sistemas y la seguridad de la información.

ISO

Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

ISO 17799

Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. Dio lugar a ISO 27002, por cambio de nomenclatura, el 1 de Julio de 2007. Ya no está en vigor.

ISO/IEC 27001

Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

ISO/IEC 27002

Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.

ISO/IEC 22301

Código de buenas prácticas como lead auditor

- **L**

Lightweight Directory Access Protocol (LDAP)

Protocolo ligero/simplificado de acceso a directorios, el cual es utilizado para permitir el acceso a un servicio en una red de comunicaciones.

Línea Base

Condiciones de configuración y parametrización que debe cumplir para su buen funcionamiento.

Lead auditor

Véase: Auditor jefe.

LPDP

Law on Personal Data Protection. Ley de protección de datos personales.

- **O**

Objetivo

(inglés: Objetive). Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

- **P**

PCI – DSS

(Ingles: Payment Card Industry Data Security Standard). Estándar de Seguridad liderado por las empresas dueñas de las franquicias de tarjetas Débito y Crédito a nivel mundial, que ayuda a las empresas a gestionar los datos de estas tarjetas de forma segura cuando procesan, almacenan y / transmiten datos de los tarjetahabientes.

Plan de continuidad del negocio

(inglés: Bussines Continuity Plan). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Proceso

(inglés: Process). Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

- **Q**

QSA

Qualified Security Assessor, utilizado como compañía independiente para hacer calificación de PCI – DSS.

- **R**

Riesgo

(inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **S**

Sarbanes-Oxley

Ley de Reforma de la Contabilidad de Compañías Públicas y Protección de los Inversores aplicada en EEUU desde 2002. Crea un consejo de supervisión independiente para supervisar a los auditores de compañías públicas y le permite a este consejo establecer normas de contabilidad, así como investigar y disciplinar a los contables. También obliga a los responsables de las empresas a garantizar la seguridad de la información financiera.

Seguridad de la información

(inglés: Information security). Preservación de la confidencialidad, integridad y disponibilidad de la información.

Sniffing

Consiste en escuchar el tráfico de la red en un modo donde se duplica los paquetes de comunicación otro equipo de comunicación. Comúnmente es realizado este proceso para monitorear tráfico de forma benéfica o maliciosa si no ha sido autorizado este proceso por el dueño de la comunicación.

SOX

Sarbanes Oxley. Ley de los Estados Unidos de América para las compañías que cotizan en Bolsa para monitorizar el valor de las acciones de la compañía y evitar su valoración dudosa.

SQL

Structured Query Language, Lenguaje de programación utilizado para programación, diseñado para administración y recuperación de datos de una base de datos relacional.

SQL Injection

Método de infiltración de código en una aplicación para obtener de forma fraudulenta datos de una Base de datos y alterar el funcionamiento normal del programa, donde no se ha autorizado a obtener esta información o administración del programa.

Superintendencia Financiera de Colombia

La Superintendencia Financiera de Colombia, es un organismo técnico adscrito al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y financiera y patrimonio propio. (Colombia, 2019)

- **T**

Tratamiento de riesgos

(inglés: Risk treatment). Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad

(inglés: Accountability). Según [CESID:1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Threat Intelligence

Plataforma de inteligencia de la amenaza que entrega información de ataques sobre la marca, exposición de información sobre una empresa, que se están informando en la dark web y deap web

- **V**

Vulnerabilidad

(inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.

- **W**

  Wrapping Attack

  Ataque de envoltura, una vulnerabilidad en los mensajes de SOAP en una comunicación web en sistemas de comunicación en la nube, donde se busca modificar el cuerpo del mensaje en la parte de la firma para suplantar la comunicación.

- **X**

  XSS

  (inglés: Cross-site scripting). Es un tipo de vulnerabilidad informática que poseen las páginas web, con el cual se puede obtener informacion que se almacena al interior de una organización o servicio en una base de datos sin poseer los permisos de acceso a esta información.