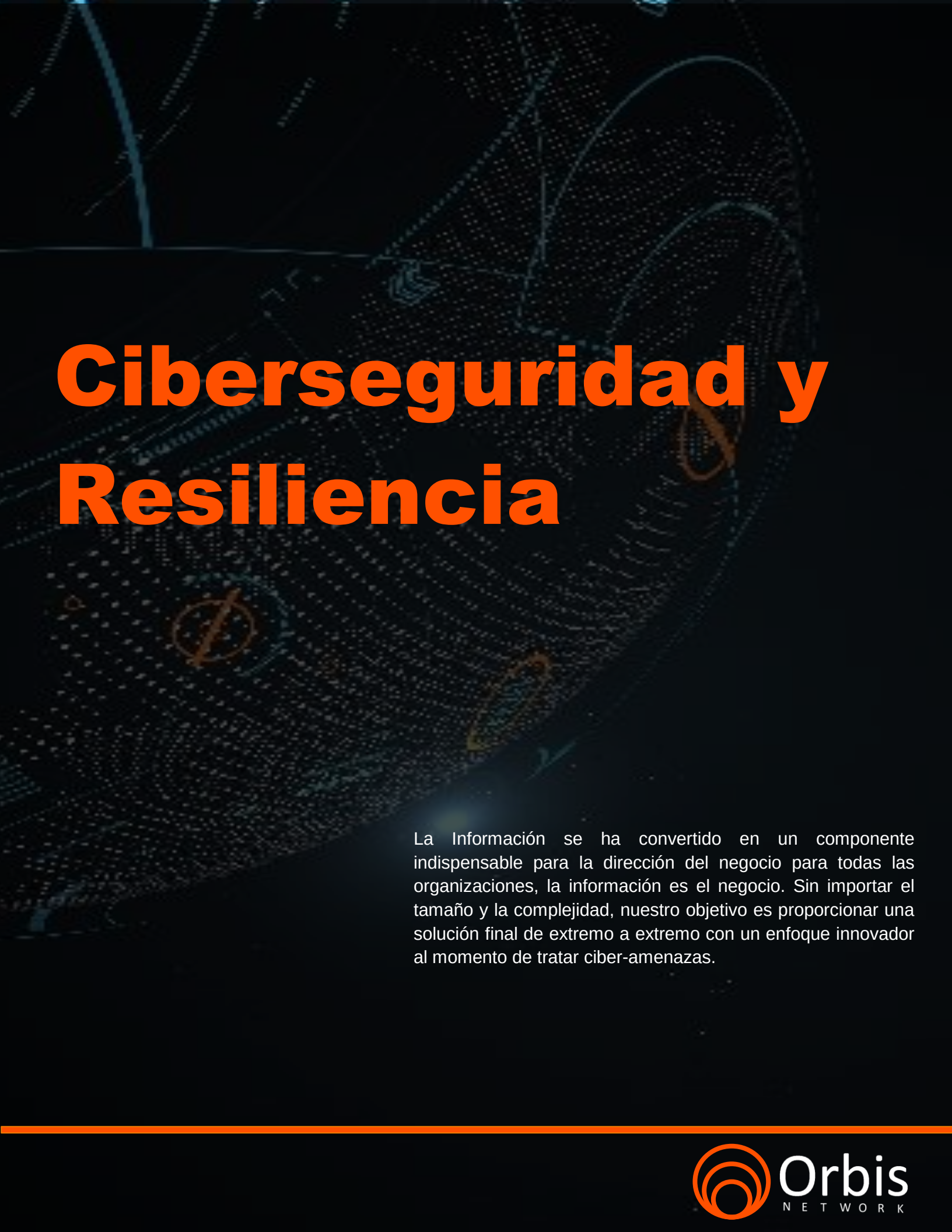

Ciberseguridad y Resiliencia

La Información se ha convertido en un componente indispensable para la dirección del negocio para todas las organizaciones, la información es el negocio. Sin importar el tamaño y la complejidad, nuestro objetivo es proporcionar una solución final de extremo a extremo con un enfoque innovador al momento de tratar ciber-amenazas.

Orbis NETWORK

Los Ciber-Criminales más buscados:

En la lista de los Cyber-criminales más buscados del FBI se encuentran un total de 17 individuos responsables por causar eventos de pérdidas desde 350.000 hasta más de 100 MM de Dólares.

https://www.fbi.gov/wanted/cyber

Insiders:

59% de los empleados internos que renuncian o son despedidos se llevan
información corporativa.

Symantec Newsroom:
https://www.symantec.com/about/newsroom

CIBERSEGURIDAD Y RESILIENCIA

SUS ACTIVOS DE INFORMACION ESTAN EN RIESGO?

Las organizaciones dependen cada vez más de la tecnología de la información para llevar a cabo sus negocios, los controles de seguridad se convierten en un elemento fundamental para el cumplimiento de sus metas. Se requieren de controles específicos cada vez más efectivos para mitigar el riesgo, que le permitan tanto al negocio, los clientes y otros grupos de interés obtener la confianza suficiente en la tecnología utilizada para lograr los objetivos planteados en términos de rentabilidad y confiabilidad.

El entendimiento de los riesgos bajo el enfoque tradicional Integridad-Disponibilidad-Confidencialidad y el saber qué hacer con estos ya no es suficiente. En **Orbis** lo ayudamos a diseñar, implementar y entregar los controles de seguridad necesarios para efectivamente reducir estos riesgos garantizando que los mismos son aptos para la finalidad que fueron concebidos, que son mantenidos de manera correcta y sostenible durante todo el ciclo de vida de la Información.

En Orbis consideramos de vital importancia la protección de sus activos de información contra amenazas percibidas. Nuestra metodología basada en riesgo les permite a las organizaciones lograr la implementación de controles administrativos, técnicos, físicos completamente integrados en el ciclo de vida de las TI, haciendo un uso eficiente de los recursos, manejando adecuadamente la incertidumbre y en cumplimiento con las mejores prácticas y regulaciones.

Nuestras Enfoque:

Nuestro conocimiento del mercado local y metodologías basadas en mejores prácticas permite, la conformación de equipos profesionales focalizados, experimentados y altamente eficientes, todos ellos con experiencia real en Medios de Pago Electrónico, garantizándole resultados exitosos.
Como profesionales dedicados a la industria de pagos y servicios financieros, nuestro objetivo principal es desarrollar e implementar las estrategias específicas que mejor se adapten a nuestros clientes y que le permitan potenciar su rendimiento operacional, expandir sus habilidades y mejorar su crecimiento. Esto es posible gracias a la optimización de los procesos, conocimientos y prácticas en su organización, todo ello bajo un enfoque de Gobierno, Riesgo y Cumplimiento (GRC).

Desarrollo de Productos y Mercado

Le ayudamos a fortalecer todo el ambiente de control y la postura de seguridad de la información enfocamos todo nuestro esfuerzo para el aprovechamiento de oportunidades a través del desarrollo de estrategias, "business cases", análisis de mercado y planes de implementación. Nuestros equipos de consultores aportan su experiencia tanto en el mercado local como el internacional para guiar y proponer a nuestros clientes soluciones comerciales, regulatorias y legales.

Diseño y Ejecución de Estrategias

Orbis facilita las metodologías necesarias a sus clientes, para que estos puedan ejecutar sus distintas estrategias de negocio en seguridad, desde el levantamiento de la información y requerimientos hasta el diseño de procesos pasando por los distintos elementos de arquitectura empresarial, gestión de proyectos, selección y/o desarrollo de los controles y la tecnología involucrada, todo ello gracias a la ejecución basada en nuestra amplia experiencia operacional y técnica.

Gestión de Riesgo, Fraude y Seguridad de la Información

Orbis aporta experiencia y liderazgo en esta exigente disciplina dentro de la industria. A través de nuestras metodologías, el conocimiento y la experiencia de nuestros consultores certificados ofrecemos soluciones que permiten que nuestros clientes puedan entender mejor, mitigar y gestionar el riesgo y sus controles asociados a través de todo el ciclo de vida de la información.

CYBERSECURITY FRAMEWORK	ANALISIS Y/O PLAN SISTEMATICO
IDENTIFICAR Evaluar Riesgos	Realizar un exhaustivo análisis de riesgos. Descubrir vulnerabilidades potenciales
PROTEGER **Desarrollar Salvaguardas**	Desarrollar políticas y procedimientos. Implementar apropiados controles de acceso, autenticación y registro.
DETECTAR **Monitoreo Continuo**	Monitoreo eficiente y definición de alertas. Habilitar registros de auditoría.
RESPONDER **Tomar Acción**	Establecer un plan de respuesta sólido. Correlacionar, analizar, clasificar y responder a eventos e incidentes detectados.
RECUPERAR **Continuidad y Resiliencia**	Implementar planes de recuperación. Aplicar mejoras para prevenir futuros ataques.

ROADMAP INICIAL

Identificar el perfil de la organización basado en su contexto externo e interno y los aspectos relevantes a la Ciberseguridad.

De la evaluación integral bajo un enfoque GRC, se generan Scorings de madurez y cumplimiento en ciberseguridad (Cybersecurity Capability Maturity Model).

Identificar las brechas en prácticas de ciberseguridad, agruparlas bajo un esquema de clasificación y priorizarlas con la finalidad de abordarlas holísticamente tomando en consideración la interdependencia de los controles involucrados.

Crear una hoja de ruta para implementar los controles basados en prioridad, complejidad, interdependencia y recursos necesarios para su diseño e implementación.

Entregar una hoja de ruta y plan de iniciativas y proyectos priorizados de alto nivel no dependiente de marcas o fabricantes específicos donde su empresa decide la estrategia de implementación. (Tercerizado, con personal interno o mixto)

.

Llegar desde donde está a donde quiere estar, sin quedar en la bancarrota.

Para mantenerse al día con las mejores prácticas internacionales y las más recientes, los corporaciones cuentan con una amplia gama de recursos de seguridad cibernética en línea; desde agencias gubernamentales, asociaciones sin fines de lucro, académicas y fabricantes, no obstante, estas fuentes de información aunque son ricas en teoría y se basan en acciones procesables que deben ser abordadas con una postura inteligente dado que; con fondos y personal limitados para invertir en nuevos esfuerzos de ciberseguridad, es necesario conocer cuáles serán las inversiones que aportarán un valor real para el negocio.

Orbis ofrece servicios profesionales de ciberseguridad diseñados para ayudar a las organizaciones a maximizar sus esfuerzos y presupuestos en ciberseguridad; que otorga visibilidad inmediata de las operaciones en relación con las mejores prácticas de la industria, identificando los elementos clave y los prioriza para que la empresa sepa donde enfocar sus inversiones.

SERVICIOS ADICIONALES

Construyendo resilencia a todos los niveles

- Desarrollo de arquitectura de seguridad en toda la empresa.
- Capacitación en materia de ciberseguridad.
- Concientización de las áreas de negocio en materia de ciberseguridad y resiliencia organizacional.
- Gobierno y gestión de seguridad de la Información.
- Gestión de Riesgos Tecnológicos y de la información.
- Resiliencia y Continuidad del Negocio.
- Auditorías de cumplimiento y evaluación de controles.
- Evaluaciones Técnicas de Seguridad de la Información.

GOBIERNO Y GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Según el IT Governance Institute (ITGI) el gobierno *es "el conjunto de responsabilidades y prácticas, ejercidas por el consejo de dirección y la dirección ejecutiva, con la finalidad de brindar una dirección estratégica, garantizar que se logren los objetivos, determinar que los riesgos se administran de forma apropiada y verificar que los recursos de la empresa se utilizan con responsabilidad."* Para la mayoría de las organizaciones, la información y el conocimiento en el que esta se basa es uno de los activos más importantes sin los cuales sería imposible dirigir el negocio. Esta creciente dependencia de las organizaciones a su información y la tecnología que la maneja, conjuntamente con los riesgos, beneficios y oportunidades que representan dicho recurso han hecho del Gobierno de Seguridad de la Información un aspecto cada vez más crucial.

El gobierno de seguridad de la información representa un componente importante y fundamental para diseñar, implementar y mantener un sistema eficaz de gestión de seguridad de la información (SGSI). A través del diseño y la implementación de un conjunto multi-disciplinario de planes estratégicos, políticas, normas, procedimientos, estándares, estructuras, procesos y otros controles para gestionar la información a un nivel empresarial, el gobierno de seguridad de la información proporciona orientación que deriva en una adecuada alineación estratégica, gestión de riesgos, entrega de valor, optimización de recursos, medición del desempeño e Integración.

Orbis cuenta con una serie de expertos en seguridad que tienen la experiencia necesaria para guiarlo a través de todo el proceso de gobierno, garantizando que los riesgos de TI, mejores prácticas y las regulaciones estén debidamente integrados en su organización y alineados con los objetivos del negocio, lo que le permite obtener un rendimiento óptimo ajustado al riesgo empresarial.

Desarrollo y Gestión de Políticas y Programas de Seguridad de la Información

Un buen programa de seguridad de la información incluye el conjunto de actividades, proyectos y/o iniciativas coordinados utilizados para implementar la estrategia de seguridad de la información y gestionar el programa lo que incluye dirigir, vigilar y monitorear las actividades relacionadas con la seguridad de la información para apoyar los objetivos de la organización. Este incluye todas las actividades y recursos necesarios que proporcionan colectivamente los servicios de seguridad de la información a la organización y que suponen el diseño, desarrollo, integración e implementación de los controles los cuales pueden variar desde simples Políticas y procesos, hasta soluciones tecnológicas de alta complejidad.

En **Orbis** podemos facilitarle los métodos y recursos necesarios para que puedan ser desarrolladas e implementadas Políticas, Normas, Procedimientos y Estándares enmarcados en programas de seguridad integrados, eficientes y rentables; así como los diferentes mecanismos necesarios para medir su desempeño de una manera práctica, incorporando los distintos elementos del marco regulatorio en un lenguaje común y entendible al negocio.

Diseño, Desarrollo y Evaluación de Arquitectura de Seguridad de la Información

Orbis le facilita los mecanismos necesarios basados en mejores prácticas (como SABSA, TOGAF, DoDAF, MODAF, entre otras) para que pueda desarrollar y mantener su propio esquema de Arquitectura de Seguridad de la Información; ya sea de manera individual o como un subconjunto de la arquitectura empresarial. Este esquema de arquitectura fundacional le servirá para desarrollar una gran variedad de arquitecturas conceptuales, lógicas, físicas funcionales y operacionales que mejor se adapten a sus necesidades, su organización tendrá la capacidad a través de un método común, de diseñar un objetivo o estado deseado que refleje e implemente las distintas estrategias del negocio en materia de seguridad, en términos de un conjunto de componentes básicos con su integración e interacción. Por otra parte, la Arquitectura Objetivo, también conocida como arquitectura de referencia le servirá de guía para establecer los objetivos más lejanos en el tiempo para el diseño técnico de sistemas y procesos.

Ingeniería Social la manera favorita para manipular víctimas:

Las personas son el eslabón más débil cuando se trata de la seguridad, una red internacional de crimen cibernético obtuvo 1 mil millones en 2 años a partir de 100 bancos en 30 diferentes países Spear fishing, el más exitoso en la Internet representan el 91 % de los ataques (Ingeniería Social).

Kapersky Labs: Carbanak APT

Social Media, los favoritos de los hackers:

Existen más de 1,6 millones de usuarios de redes sociales en todo el mundo, más del 64 % de los usuarios de Internet que accedan a los servicios de redes sociales en línea. Más de 600.000 cuentas de facebook son hackeadas cada día.

http://www.statista.com/

Gestión de Riesgos de la Información

La gestión de riesgos establece las distintas actividades coordinadas destinadas a dirigir y controlar una organización en lo concerniente al riesgo; el riesgo es un factor influyente y debe ser evaluado en todos los niveles de la organización: estratégicos, unidades de negocio y sistemas de información, el mismo puede considerarse como un obstáculo para el logro de objetivos de una organización.

La gestión de riesgos de la información es la aplicación sistemática de las políticas, procedimientos y prácticas de gestión a las tareas de identificar, analizar, evaluar, informar tratar y monitorear el riesgo relacionado con la información.

Evaluación de Riesgos

Mediante nuestra metodología para la gestión de riesgos realizamos evaluaciones de riesgos integrales, cuyo objetivo le proporcionará una serie de guías y recomendaciones que maximicen la protección de los activos de información críticos de su organización en términos de confidencialidad, integridad y disponibilidad, asegurando que sus riesgos y oportunidades relacionados con la TI estén debidamente identificados, analizados, tratados, monitoreados y presentados en términos del negocio.

Inventario y Clasificación de Activos

Las mejores prácticas en su mayoría (ISO/IEC 27005, ISO/IEC 31000, Nist SP 800-30, TRA, Octave, entre otras) requieren que las organizaciones protejan y gestionen sus activos de TI críticos de manera adecuada, a través de nuestras soluciones su organización podrá desarrollar una metodología para el inventario y la clasificación de activos con la finalidad de proteger su información, para esto es esencial: Definir la propiedad de activos, su uso adecuado, tipificarlos mediante un esquema de clasificación; así como, identificar las distintas medidas de protección y manipulación de los mismos.

Un inventario de activos debe incluir los elementos lógicos y físicos de la infraestructura de información, debe incluir las ubicaciones y servicios de apoyo, sus procesos de negocio asociados y la clasificación de los datos para cada elemento de datos. Igualmente debe identificar las características de los datos esenciales que deben ser protegidos, el nivel de sensibilidad y cualquier otra información relacionada a activos críticos identificados por su organización.

La mayoría de las pérdidas son irrecuperables:

Según estudios realizados el tiempo promedio para detectar un ataque fue de 170 días. En el caso del sector bancario del total de las pérdidas reportadas, un 68% se considera irrecuperable.

Ponemon Institute:
http://www.ponemon.org/index.php

Infosecurity Magazine:
http://www.infosecurity-magazine.com/view17194/banksfailing-to-detect-and-stop-online-fraud-before-it-happens/

3,8$ Millones — **Es el costo promedio de una fuga mayor de datos de una compañía.**

Microsoft Advanced Threat Analytics

146 DIAS — **Es el tiempo promedio que un atacante permanece en una red antes de ser detectado.**

Microsoft Advanced Threat Analytics

60% RESCATES — **De pagos por Malware en el 1er. Cuarto del 2017 fue por Ramsomware.**

Malwarebytes

Cumplimiento y Evaluación de Controles

Identifique y logre implementar de una manera rápida, sencilla y transparente todos los controles necesarios para dar cumplimiento tanto a las regulaciones como a mejores prácticas y estándares en materia de Seguridad de la Información. **Orbis** integra los controles necesarios en los distintos marcos de trabajo para dar cumplimiento a las distintas regulaciones.

Nuestros consultores certificados y con años de experiencia en materia de cumplimiento normativo le ayudaran a determinar con claridad los aspectos mínimos necesarios para lograr el cumplimiento. Nuestros expertos en materia de seguridad y riesgo han participado en el diseño y elaboración de distintas normativas y resoluciones en Venezuela; también cuentan con las certificaciones y experiencia en campo en lo que a la evaluación de cumplimiento normativo se refiere.

Le ayudamos a identificar brechas y requerimientos de cumplimiento en base a los mejores marcos o estándares nacionales e internacionales:

- PCI DSS
- ISO/IEC 27000
- Cobit
- ITIL
- TOGAF
- NIST 800-53

Capacitación y Concientización

La capacitación y concientización son elementos fundamentales para que cualquier iniciativa de seguridad se lleve a cabo de manera exitosa. A través del diseño e implementación de planes de capacitación y concientización en materia de seguridad y controles su organización puede lograr un cambio positivo en el comportamiento de las distintas partes interesadas lo que ayudará a enfrentar con una mejor postura las distintas amenazas planteadas.

Nuestros instructores en materia de seguridad de la información emplearan todo su esfuerzo y conocimiento basado en las mejores prácticas de la industria para proporcionarle información actualizada, útil y práctica sobre cómo mejorar la postura de seguridad de la organización lo que se traduce en un mejor trato hacia las amenazas conocidas y emergentes.

EVALUACIONES TÉCNICAS DE SEGURIDAD DE LA INFORMACIÓN

En la actualidad los ataques se tornan cada vez más creativos y sofisticados, estos pueden tomar gran cantidad de formas y causar graves consecuencias. Los negocios pueden ser afectados por la pérdida o substracción de información confidencial y/o de propiedad intelectual; las operaciones del estado llevadas a cabo por instituciones tanto públicas como privadas pueden verse comprometidas; los sistemas de control de infraestructuras críticas como las redes eléctricas y de telecomunicaciones pueden interrumpir sus servicios debido a brechas en la seguridad.

A través de nuestras auditorías técnicas de seguridad de seguridad el personal de su organización podrá obtener las respuestas y recomendaciones necesarias para mejorar el nivel de seguridad y proteger los activos más valiosos de su organización. Nuestros servicios de auditorías técnicas de seguridad detectan vulnerabilidades y descubren debilidades presentes en los procesos de seguridad de la organización que pueden ser utilizadas por usuarios no autorizados.

Estas evaluaciones son llevadas a cabo por nuestros consultores certificados en seguridad (ethical hackers) que simulan ataques mediante el uso de las mismas técnicas que un atacante malintencionado utilizaría. El objetivo de esta auditoría es evaluar si la estructura de información de su organización puede ser accedida fácilmente sin autorización o no.

Orbis le ayudará a determinar con claridad lo que hay que hacer para que su organización proteja los activos críticos de TI, siguiendo las estrategias especializadas en las mejores prácticas reconocidas de la industria.

Test de Penetración

Los Test de penetración simulan un ataque real contra su infraestructura en un entorno controlado, que permite evaluar la capacidad de su arquitectura de seguridad de evitar tipos particulares de ataques. Nuestras pruebas se llevan a cabo empleando las mismas técnicas que un atacante (ya sea interno o externo a su infraestructura) pueda realizar y verifican, sin revelar demasiada información de su entorno: si los servidores o aplicaciones serían resistentes a distintos tipos de ataques hostiles y si las vulnerabilidades identificadas pueden conducir a una mayor intrusión y explotación. Las pruebas de penetración también incluyen pruebas de penetración de red y pruebas de seguridad de aplicaciones, así como de los controles y procesos que giran en torno a estos.

Nuestros Test de penetración están diseñados para simular un ataque real contra su infraestructura en un entorno controlado. Es el primer paso para identificar que tan seguro se encuentran sus activos tecnológicos. El informe final le ayudará a entender su actual postura de seguridad y le proporcionará recomendaciones sobre cómo mejorar su defensa frente a las vulnerabilidades tecnológicas que pueden conducir a las intrusiones, el fraude y las interrupciones del servicio. Más allá de un listado de vulnerabilidades generado por un gran conjunto de herramientas, le aportamos el valor agregado que le permitirá abordar de manera priorizada un plan de acción eficiente y rentable y con una perspectiva adicional enfocada al cumplimiento de los distintos elementos del marco normativo.

Evaluación de Aplicaciones

Las organizaciones bien informadas entienden que sus aplicaciones y sitios web son algo más que un servicio de información; estos también representan y transmiten la imagen corporativa a sus clientes y el público en general.

El aseguramiento de sus sitios o aplicaciones web puede disuadir a gran parte de las amenazas de Internet, lo que se traduce en que su organización puede seguir brindando el servicio de calidad que requieren sus clientes y no gastar tiempo y dinero de manera reactiva ante una pérdida de datos o de disponibilidad. La evaluación de aplicaciones Web de **Orbis** le ayudará a comprender plenamente las vulnerabilidades presentes en las aplicaciones en línea, ya sea para un sitio web público que brinda servicio a sus clientes, una interfaz con un proveedor de servicios corporativos o un sistema interno de gestión.

Nuestros servicios de evaluación de aplicaciones web van más allá de un conjunto de pruebas automatizadas; este profundiza en los distintos controles a nivel de la lógica de la aplicación y de seguridad en los procesos de control que giran en torno a esta; así como en los distintos elementos regulatorios presentes.

Resiliencia y Continuidad del Negocio

Nuestro enfoque centrado en riesgo, el impacto, disponibilidad y capacidad de recuperación, le facilita los mecanismos personalizadas para que su organización pueda entender los desafíos específicos de continuidad de negocio mejorando su estrategia de resistencia y recuperación a nivel empresarial y logrando los objetivos de negocio y de TI. Le ayudamos a desarrollar e implementar una estrategia personalizada para hacer frente a los problemas de capacidad de recuperación de TI. Identificamos múltiples opciones para que pueda seleccionar la mejor solución a nivel de continuidad de su negocio y de resiliencia.

Diseñe y desarrolle una arquitectura flexible que apoye sus objetivos de recuperación y que fortalezca su infraestructura de TI; permita a su organización aumentar su capacidad de respuesta, con los recursos óptimos al crear un diseño de arquitectura resistente, rentable que maximice sus inversiones; al mismo tiempo implemente una estructura de gobierno que le permita satisfacer las demandas de los reguladores.

Gestión de Incidentes

Las organizaciones necesitan establecer los mecanismos adecuados que le otorguen la capacidad para gestionar efectivamente todos aquellos eventos perjudiciales e inesperados con el objeto de minimizar los impactos y mantener o restaurar las operaciones dentro de los límites de tiempo esperados por el negocio. La gestión de incidentes se considera parte operativa de la gestión de riesgos y se enfoca tanto a minimizar la ocurrencia o reducir el impacto resultante de un fallo, error o actividad malintencionada, es complementaria a la Gestión de Incidentes de TI y a los procesos de Continuidad del Negocio.

A través de nuestra metodología, la organización podrá construir planes y procedimientos de gestión y respuesta ante incidentes que permitan:

- Detectar Incidentes rápidamente.
- Diagnosticar Incidentes con Exactitud.
- Gestionar Incidentes adecuadamente.
- Reducir y minimizar los daños.
- Restaurar los servicios afectados.
- Determinar las causas originales.
- Implementar mejoras para evitar que se repitan.

Entendiendo el Impacto financiero y reputacional del ITRisk:

Fuente: Ponemon Institute / IBM

BENEFICIOS

- Identificación y mitigación de ciber-amenazas que enfrentan a la organización.
- Maximizar el retorno de la inversión en Seguridad de la Información.
- Eficiencia estratégica y operacional a la hora de seleccionar y mantener Soluciones basadas en Seguridad.
- Aumento de la confianza de los ejecutivos, reguladores y otros stakeholders al demostrar que el riesgo está siendo efectivamente manejado y los objetivos de seguridad están siendo cumplidos.
- Asegurar el cumplimiento de los requerimientos regulatorios y la alineación con las mejores prácticas.
- Lograr que su programa operacional de seguridad siga siendo sostenible a largo plazo, con un enfoque en la mejora continua y con la debida alineación continua con los objetivos del negocio.
- Fortalecer la postura de Seguridad de la Información de la organización y Priorizar a los requisitos de seguridad en Tecnología para centrar su inversión en donde tendrá el mayor impacto.
- Incrementar la concientización lo que le permitirá tomar decisiones informadas sobre cómo manejar los riesgos; focalizar el gasto, evitar impactos, y gestionar los riesgos a un nivel aceptable bajo un enfoque proactivo.
- Preservar la Imagen Corporativa y la Lealtad de los clientes al mejorar la capacidad de recuperación y optimizar la continuidad del negocio.
- Esquemas de Seguridad basados en optimización de costos y entrega de valor.
- Diseño e Implementación de procesos de control y arquitectura de Seguridad.
- Evaluación e Implementación de un framework de Seguridad basado en procesos de negocio.

¿Cómo podemos ayudarle?

Conozca más acerca de cómo nuestras soluciones de Seguridad de la Información basadas en GRC pueden ayudarlo a brindar valor y transformar su negocio con un mínimo de costo y riesgo:

- Diseñar, Implementar y formalizar las distintas estrategias y programas de ciberseguridad.
- Desarrollo de Productos y Servicios de seguridad basados en optimización de costos y entrega de valor.
- Ejecución de Pruebas de Penetración a la medida de sus necesidades.
- Ejecución de Evaluaciones de Riesgo, Evaluaciones de Amenazas, Evaluaciones de Vulnerabilidades, Inventario y Clasificación de activos.
- Elaboración de Análisis de Impacto de Privacidad (PIA).
- Modelado de Procesos de Negocio, y Gestión Documental.
- Construcción de Políticas, Normas, Procedimientos y Estándares en Seguridad de la Información.
- Auditoría y Evaluación de Cumplimiento PCI-DSS, PA-DSS, Nist CSF, ISO/IEC 27001, Cobit y/o del Marco Regulatorio aplicable.
- Implementación de Metodologías de Gobierno y Arquitectura Empresarial basadas en Seguridad de la Información.
- Diseño y elaboración de procesos de Gestión de Incidentes.
- Modelado de Escenarios y Casos de Negocio.
- Proyectos de Innovación Tecnológica para su negocio.
- Construcción de Indicadores, Gestión de Calidad y Desempeño aplicable a procesos de Control.
- Elaboración de Análisis de Impacto al Negocio, Planes de Continuidad de Negocio (BCP) y Planes de Recuperación de Desastres (DRP)

Tecnología de punta de última generación

Nuestras soluciones de Seguridad se implementan sobre una arquitectura tecnológica fundamentada bajo un enfoque de GRC. A través de nuestros Partners facilitamos la tecnología de punta que mejor se adapta a sus necesidades, permitiendo soportar y complementar nuestras metodologías y potenciando la gama de posibilidades que se traducen en mejores resultados y aporte de valor a su negocio. Las soluciones tecnológicas adquiridas través de nuestros Partners, su proveedor de confianza o a partir de un esquema mixto son incorporadas en un marco de gestión de riesgo y en cumplimiento con las mejores prácticas y regulaciones locales, podemos ayudarle a desarrollar o adquirir la solución automatizada que necesita para asegurar su negocio.

Por qué Orbis?

Contamos con un equipo de profesionales de alto nivel que han liderado con éxito numerosos proyectos regulatorios para organizaciones que requieren de licencias bancarias, de instituciones o miembros de redes de pago (Vg.: Visa o MasterCard). Nuestros expertos han participado en la elaboración de regulaciones en materia de Seguridad de la Información y tienen el conocimiento específico de marco regulatorio vigente, la experiencia y el "know-how" operacional para garantizar el éxito de la obtención de las licencias o permisos requeridos.

Expertos en Estrategias Controles y Regulaciones

Ya sea para ayudarle a establecer su marco estratégico, analizar las oportunidades del mercado o diseñar el marco de control adecuado **Orbis** aporta gran experiencia y conocimiento específico en materia de ciber-seguridad. Los diferenciadores claves de Orbis son el profundo entendimiento de las regulaciones de parte de nuestros consultores, quienes lideraron su elaboración y la evaluación de los distintos marcos regulatorios vigentes.

Conocimiento del Mercado

Con un conocimiento del mercado a lo largo de toda la cadena de valor, **Orbis** ha ayudado con éxito a sus clientes aportando conocimientos específicos del sector e impulsando a las organizaciones a moverse en mercados paralelos o ampliar su rango de productos, así como a abordar otros sectores. En **Orbis**, estamos orgullosos de tener un buen acercamiento a los mercados y conocer de primera mano el amplio abanico de productos para ayudar a diseñar e implementar planes efectivos de entrada a nuevos mercados y ayudarles a alcanzar sus objetivos de negocios.

Entrega de Proyectos

Orbis ha construido una gran reputación en la entrega de resultados. Esto ha sido posible gracias a nuestra experiencia en el sector y a la entrega de soluciones de calidad, para entregar al cliente los resultados esperados. Desde la selección de proveedores/productos y la tecnología asociada, **Orbis** posee la técnica y conocimientos para mitigar los riesgos y asegurar el éxito de proyectos en el área de medios de pago.

Eficacia Operacional

Orbis trabaja con sus clientes para mejorar su eficiencia operacional a través de reducción de costos, desarrollo de procesos más agiles y mejoras en la obtención de ingresos aportando un valor real a su negocio. Desde la evaluación comparativa del rendimiento, esquemas de reducción de costes a través de eficiencias operacionales, **Orbis** posee una dilatada experiencia operacional, datos de rendimiento y una metodología de procesos para ayudar a las organizaciones a conseguir sus objetivos de negocio.

Orbis
NETWORK

Contáctenos

www.orbisnetwork.com.ve

contact@orbisnetwork.com.ve