Forensic CORP
PREVENTION AND RESPONSE

Consultoría Estratégica

Los servicios que hemos diseñado buscan satisfacer el ciclo de implementación de cualquier norma o plan estratégico, involucrándonos en las etapas de diagnostico inicial de un proyecto de seguridad, servicios TI y plan antifraude, así como también durante su operación y evaluación. Cuando un incidente ocurra, su organización estará preparada para reaccionar ante eventos que puedan afectar su patrimonio y evitar su recurrencia en el futuro.

- Contamos con un grupo multidisciplinario, con profesionales de vasta experiencia en el ámbito normativo de la seguridad de la información, fraudes corporativos y gestión de los servicios TI, diseñando soluciones que integren la gestión eficiente, con la tecnología eficaz que permiten la correcta implementación de controles que minimicen los riesgos a los cuales se puede ver expuesta su organización.

- Apoyamos a nuestros clientes en cada una de las etapas o fases de proyectos de implementación técnica y/o normativa, a través de servicios específicos que pueden abordar la realización total o parcial, focalizadas en satisfacer las necesidades de la organización.

- Nuestros servicios entregan resultados específicos a nuestros clientes, ya que vendemos resultados, ante lo cual buscamos asegurar un producto de calidad y que sea de real utilidad a la organización, los cuales buscan satisfacer los objetivos y requerimientos planteados para dicho proyecto.

FC

Desafíos

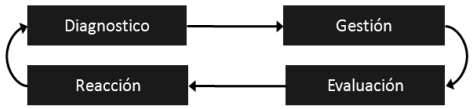
- La organización ha experimentado o teme por una violación de seguridad informática.
- Los desarrollos de software no son controlados y teme por la fuga de información estratégica o confidencial.
- El daño a la compañía y su reputación, por el robo de información confidencial de los clientes y la compañía.
- Desconocimiento de los incidentes existentes, el estado actual de seguridad, riesgos y amenazas, siendo la seguridad impulsada de manera reactiva frente a la proactiva.
- La inoperatividad prolongada de la compañía por incidentes críticos o catástrofes pueden afectar considerablemente su patrimonio, generando perdida financiera directa o perdida de valor de mercado.
- Su organización no esta preparada para operar e incluso sobrevivir ante eventos catastróficos que afecten su información estratégica.
- Por una deficiente estructuración de los procesos que gestionan los servicios tecnológicos, se ve mermada la confianza de los clientes en relación a la calidad de los servicios TI prestados.
- Su empresa es victima de fraudes internos y externos, afectando su patrimonio, ante lo cual la organización no cuenta con las herramientas y procesos para su prevención y detección.
- Fallas en los programas de pruebas para validar planes de continuidad y promover su operación eficiente a conciencia por parte de los empleados.

Ventajas

- Identificar proactivamente las amenazas y gestionar el riesgo.
- Proteger la disponibilidad, confidencialidad e integridad de la información corporativa aplicando controles pertinentes.
- Proteger la compañía, su reputación y confianza de los clientes.
- Establecer las directrices necesarias para evitar introducir a las aplicaciones, vulnerabilidades adicionales durante sus desarrollos, instaurando un proceso de desarrollo seguro.
- Evaluación de estado actual de la organización que permita decidir en base a la evaluación de riesgos críticos de seguridad, operatividad o insatisfacción de los clientes, enfocarse en generar planes de acción en las áreas criticas o relevantes para la organización.
- Alineación del la gestión de la continuidad del negocio (BCM) a la estrategia organizacional.
- Proteger el flujo de ingresos y servicios de la compañía, disminuyendo perdidas importantes para la organización, a través de la implementación de procesos y herramientas que prevengan hechos fraudulentos por parte de personas internas y externas a la organización.
- Proteger a su organización de fraudes instaurando procesos de control y gestión que permitan detectar, analizar, desincentivar y mitigar hechos delictivos.
- Ventajas competitivas ante la competencia por el valor agregado de los productos y/o servicios ofrecidos.

Servicios

Los servicios que colocamos a disposición de nuestros clientes se han categorizado de acuerdo a su finalidad y etapa en la cual intervienen dentro de los procesos de implementación de los proyectos de seguridad y/o tecnológicos de nuestros clientes.



Nuestros servicios integrales permiten a nuestros clientes mejorar deficiencias en el diseño de su seguridad y servicios que pueden llevar a accesos no autorizados y destrucción de información estratégica, a través de la identificación y gestión de riesgos logrando controlar las amenazas que pueden afectar sus activos de información e inoperatividad asegurando el funcionamiento de sus servicios y actividades claves a un nivel aceptable cuando se deba trabajar en contingencia.

Diagnostico	**Gap Análisis** **Análisis de Riesgos**
Gestión	**Implementación de Sistemas de Gestión** **Implementación de Planes Estratégicos** **Implementación Tecnológica** **Capacitación y Concientización**
Evaluación	**Auditorias Internas y Externas** **Evaluación de Controles**
Reacción	**Investigación Tecnológica** **Investigación de Fraude**

http://www.forensiccorp.cl Av. Los Militares Nº 5620, Oficina 1011 Piso 10, Las Condes, Chile Teléfono +562 2896 63442, contacto@forensiccorp.cl

Cybersecurity
FORENSIC SECURITY FOR ENTERPRISE

Forensic Investigation
FORENSIC COMPUTING FOR ENTERPRISE

Diagnóstico

GAP Análisis. Corresponde a un diagnostico de "Nivel de Cumplimiento Normativo" para las organizaciones que poseen interés en implementar normativas técnicas o de gestión pueden tener la necesidad de determinar el nivel de cumplimiento de los requisitos establecidos por estas, con el fin de identificar la brecha existente entre su estado actual y el óptimo. Las normas asociadas a este servicio son:

- **ISO/IEC 27001:2013**, Information security management systems, Requirements.
- **ISO/IEC 27002:2013**, Code of practice for information security controls.
- **ISO/IEC 22301:2012**, Business continuity management systems, Requirements.
- **ISO/IEC 20000:2011**, Service management, Part 1: Service management system requirements.
- **CCM V3.0.1**, Cloud Security Alliance, Cloud Controls Matrix.

Análisis de Riesgos. Este servicio permite identificar los eventos y las situaciones que pueden afectar de manera adversa a las áreas de negocio y sus procesos, a través de la evaluación de probabilidades de ocurrencia e impacto (consecuencias) de dichos eventos en la organización. Una etapa primordial dentro del Análisis de Riesgos, es el denominado "Análisis de Vulnerabilidades", por lo que el cliente puede optar por las siguientes alternativas de análisis:

- **Análisis General de Vulnerabilidades**. Corresponde a un análisis de alto nivel de las distintas vulnerabilidades que pueden afectar los activos, de acuerdo a los últimos reportes generados por la industria.
- **Análisis Técnico de Vulnerabilidades**. Corresponde a un análisis de bajo nivel, realizando una evaluación de cada unas de las vulnerabilidades que puedan afectar a los activos, la cual se realiza utilizando herramientas técnicas de verificación y evaluación.

Gestión

Implementación Sistema de Gestión. Corresponde a la implementación de procesos de operación, monitoreo y mejora continua que conlleven la disminución a un nivel aceptable de los riesgos a los cuales se ven afectados los activos de la empresa, a través de la elaboración de políticas, normas, procedimientos e instructivos que permitan su utilización. Dependiendo de los objetivos y necesidades de los clientes se ofrece la implementación de las siguientes normativas internacionales:

- **ISO/IEC 27001:2013**, Information security management systems, Requirements.
- **ISO/IEC 22301:2012**, Business continuity management systems, Requirements.
- **ISO/IEC 20000:2011**, Service management, Part 1: Service management system requirements.
- **CCM V3.0.1**, Cloud Security Alliance, Cloud Controls Matrix.

Implementación Plan Estratégico. Corresponde a la implementación de un marco de trabajo (framework) basado en buenas prácticas establecidas por normas internacionales, que permita a la organización establecer procesos de operación, monitoreo y mejora continua, que cumplan con los requerimientos específicos establecidos por la organización, basados en normativas internacionales:

- **Plan de Continuidad del Negocio**, Norma ISO/IEC 27031:2011, Guidelines for information and communication technology readiness for business continuity.
- **Plan de Seguridad Informática**, Norma ISO/IEC 27032:2012, Guidelines for Cybersecurity.
- **Plan de AntiFraude**, Norma AS-8001:2008, Australian Standard, Fraud and corruption control.

Implementación Tecnológica. Corresponde a un servicio de implementación técnica, con el cual se diseña y estructura una solución especifica a medida de las necesidades del cliente, con el fin de satisfacer los requerimientos de seguridad o de calidad de los servicios TI. El nivel y envergadura de implementación puede estar relacionado directamente con los controles establecidos por los Sistemas de Gestión o por necesidades específicas de los clientes (p.e. Planes estratégicos, Leyes, Normativas Internas, incidentes detectados, etc.). Los servicios específicos que se pueden implementar son:

- Seguridad Perimetral, Interna, Avanzada y Móvil.
- Servicios Administrados.
- Soporte Técnico Especializado
- Redes de Comunicación.

Capacitación y Concientización. Entregamos capacitaciones integrales en el ámbito de la seguridad de la información, continuidad operacional, fraude corporativo y ciencias forenses, dictados por profesionales con años de experiencia:

- Introducción a la seguridad de la información
- Gestión de riesgos, aplicado al sistema de gestión de la información bajo ISO 27001
- Implementación ISO 27001:2013
- Auditor interno ISO 27001:2013
- Prevención, detección y reacción ante fraudes corporativos
- Prevención, detección y reacción ante delitos cibernéticos
- Manejo de incidentes y evidencias digitales bajo ISO 27035 e ISO 27037
- Análisis forense informático
- Análisis forense contable
- Análisis forense en Documentoscopía y Grafología
- Análisis forense en Huellografía y Dactiloscopia

Evaluación

Auditorías Internas y Externas. Corresponde a un servicio que busca realizar una auditoría de cumplimiento normativo (a la propia organización o a proveedores), a través de la aplicación de un proceso sistemático, independiente y documentado que permita obtener evidencia de la operación del sistema de gestión implementados y evaluarla objetivamente para determinar la medida en la cual se cumplen los criterios de auditoría propuestos (objetivos de la auditoria). Los sistemas de gestión que pueden ser auditados por Forensic-Corp son los siguientes:

- **ISO/IEC 27001:2013**, Information security management systems, Requirements.
- **ISO/IEC 22301:2012,** Business continuity management systems, Requirements.
- **ISO/IEC 20000:2011**, Service management, Part 1: Service management system requirements.

Evaluación de Controles. Este servicio posee por objetivo realizar una evaluación técnica operativa de la efectividad de los controles implementados en la organización, contrastando su efectividad con las buenas prácticas establecidas por normas internacionales. Para ello se definen dos etapas fundamentales para la ejecución del proyecto:

- **Pruebas de Penetración (Hacking Ético)**. Se realizan ejercicios de penetración a distintos activos señalados por el cliente o al azar, con el fin de explotar distintas vulnerabilidades o brechas de seguridad a las cuales se puedan ver afectados, con el objetivo de obtener evidencia para realizar un análisis posterior.
- **Análisis de Efectividad de Controles**. Una vez realizadas las distintas actividades planificadas para colocar a prueba los controles establecidos, se procede a realizar una evaluación de la efectividad de los controles implementados por la organización, así como también se determinan recomendaciones para evitar los hallazgos de importancia identificados, minimizando los riesgos de que incidentes similares se vuelvan a producir.

Reacción

Investigación Tecnológica. Realizar investigaciones forenses en organizaciones que necesiten aclarar hechos que pueden ser constitutivos de delito o faltas a reglamentos internos, aplicando técnicas criminalísticas asociadas a la informática y telecomunicaciones, realizando levantamiento de evidencias y análisis forenses especializados, los cuales permitan determinar modus operandi y eventuales responsabilidades de personas. Para ello contamos con dos áreas fundamentales, que se complementan para obtener las evidencias necesarias para aclarar los hechos investigados:

- **Informática Forense**: Nuestra área de Informática Forense presta servicios especializados en el ámbito de los delitos informáticos y computacionales.
- **Telemática Forense**: El área de Telecomunicaciones se complementa con el área informática, lo cual nos permite la entrega de servicios especializados asociados con dispositivos móviles y redes de datos

Investigación de Fraudes. Realizar investigaciones forenses multidisciplinarias en organizaciones que necesiten aclarar hechos delictuales que afectan su patrimonio, aplicando técnicas forenses especializadas en el ámbito criminalístico, las cuales en su conjunto aporten antecedentes necesarios para dar sustento a investigaciones internas y/o denuncias judiciales en contra de dichas personas. Dichos resultados pueden ser utilizados para la detección e implementación de oportunidades de mejora, que permitan disminuir la probabilidad de ocurrencia de hechos delictuales o faltas a las políticas organizacionales futuras. Las especialidades con las que cuenta nuestra organización son las siguientes:

- Peritos Informáticos.
- Peritos Electrónicos y Telecomunicaciones.
- Peritos Contables.
- Peritos Documentoscópicos y Grafológicos.
- Peritos en Huellografía y Dactiloscopia.