



# TECNOLOGÍAS LEGALES INTELIGENTES

«La información es poder»

«Quién tiene la información, tiene el poder»

«Quién tiene el conocimiento sobre el conocimiento,  
tiene el poder»

## **TECNOLOGIAS LEGALES INTELIGENTES**

### **LEY INFORMÁTICA INTELIGENTE (Blockchain asistidas por humanos)**

### **ASPECTOS LEGALES EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACION**

### **COMPLIANCE EN TECNOLOGÍAS DE LA INFORMACIÓN**

### **INFORMÁTICA FORENSE – ANÁLISIS E INTERPRETACIÓN DE LA EVIDENCIA DIGITAL**

### **ANÁLISIS DE VULNERABILIDADES, RIESGOS E INCIDENTES LEGALES EN EL ENTORNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN (HACKING ÉTICO EN IT-LEGAL V1.1)**

## PROPUESTA DE SERVICIOS

### 1. NOMBRE DEL PROYECTO.

---

Tecnologías Legales Inteligentes

### 2. PLANTEAMIENTO DEL PROBLEMA.

---

Constantes problemas tecnológicos, incidentes de seguridad, interrupciones del servicio, potenciales violaciones a la ley civil y penal, sistemas vulnerables a agresiones o fallos tecnológicos, problemas de confidencialidad, accesos no autorizados, Delitos Informáticos (CP); Ilícitos Informáticos; Contratos lesivos en TI; Afectación a la Billetera Digital; Pérdida patrimonial; Empleados deshonestos; Robo de información; Mail anónimos y agresivos; Extorsiones y Suplantación de Identidad; Espionaje Tecnológico; Fraude Corporativo; Pornografía; Libertinaje Digital; Acoso Sexual, entre otros.

- Recursos Humanos (persona digital), qué, por conocimiento o desconocimiento tecnológico generan problemas y caos en el entorno de las Tecnologías de la Información.
- Estructura de Tecnologías de la Información débil, vulnerable y manipulable para el beneficio particular;
- El área de Tecnologías de la Información permite a los usuarios abusar de los recursos tecnológicos en contra de los intereses de la organización.
- Transmisión de virus, bombas digitales, ransomware, troyanos, spyware, Software Malicioso, entre otros

#### **SEGURIDAD EN Tecnologías de la Información:**

**Tercerizada.** «Exposición del conocimiento, con transferencia del know how corporativo»; **Gratis.** «No existe, mejor ignorarla porque en mi empresa no se necesita»; **Barata.** «Mal hecha, pésima configuración, vulnerable y propensa al fraude»; **Inexistente.** «Señal roja ...»; **Improvisada.** «No cuenta con recursos financieros, no cuenta con personal capacitado»; **Indiferente.** «No importa cómo funciona o si funciona».

**Teléfono Inteligente Sincronizado con los recursos, herramientas, servicios de las Tecnologías de la Información a nivel CORPORATIVO** (Teletrabajo, Email corporativo, Sistema Financiero, Recursos Tecnológicos, Redes Sociales, ...).

El área de Tecnologías de la Información, no garantiza el normal desarrollo tecnológico de la organización, continuidad del negocio, tampoco garantiza la confiabilidad al 100% de la eficiencia y eficacia de los recursos tecnológicos en la Intranet e Internet.

Además, la entidad Corporativa, pierde recursos económicos en la producción de servicios que es administrada por los recursos tecnológicos.

**En síntesis, una amplia gama de problemas en el entorno a las tecnologías de la información; problemas, que evolucionan al mismo ritmo que evolucionan las tecnologías de la información. ESE ES UN PROBLEMA QUE SE DEBE RESOLVER.**

### 3. ORIGEN Y JUSTIFICACIÓN DE LA PROPUESTA.

---

Como en todas partes del mundo, el área de Tecnologías de la Información se constituye como el instrumento gerencial imprescindible y necesario para el éxito de la gestión administrativa y empresarial, ofreciendo información eficiente, oportuna, real y confiable para la adecuada toma de decisiones; por tanto, ésta debe ser tratada y resguardada de manera muy especial, bajo modelos de Seguridad altamente confiables.

Sin embargo, estos modelos de seguridad muchas veces son afectados y vulnerados por los propios Recursos Humanos institucionales, **quienes, con dolo o culpa, con voluntad o involuntariamente, con o sin conocimiento tecnológico o por motivaciones de venganza** causan daño contra la infraestructura tecnológica, billetera digital, patrimonio institucional, contra la imagen corporativa y personal de la organización.

En síntesis, ***el área de Tecnologías de la Información se constituye como el principal activo dentro de la organización, y por supuesto, en el objetivo de todos los ataques internos y externos.***

### 4. BREVE DESCRIPCIÓN DE LA PROPUESTA.

---

En la actualidad, los alarmantes ataques internos y externos contra las Tecnologías de la Información reflejan cuantiosas pérdidas económicas, falta de credibilidad, pérdida de confiabilidad, contaminación de los registros electrónicos y otras contingencias a causa de las diversas Vulnerabilidades y Riesgos en el entorno legal de las Tecnologías de la Información.

La mayor frecuencia de pérdidas económicas, está orientada a: i) falta de conocimiento de los RRHH en el uso adecuado de los recursos Tecnológicos, ii) TI desprovistas de nomenclaturas legales en la Intranet e Internet, iii) exceso de confianza en el alcance del Software de seguridad, iv) tercerización de servicios, y v) el área de Tecnologías de la Información, orienta sus principales actividades a la implementación de parches de seguridad que no ofrecen ninguna seguridad tecnológica. Razones que derivan en el libertinaje digital, fraude corporativo, pérdidas económicas y otras acciones que atentan contra la estabilidad corporativa.

En conclusión, la propuesta está diseñada para establecer e implementar mecanismos legales que permitan garantizar y maximizar el aseguramiento de todo el entorno de las Tecnologías de la Información, y lograr que la entidad corporativa recupere las pérdidas económicas y fortalezca la imagen corporativa.

### 5. OBJETIVO.

---

Asegurar AL 100% LAS TECNOLOGÍAS DE LA INFORMACIÓN MEDIANTE LA IMPLEMENTACIÓN Y CONSTRUCCIÓN DE SOLUCIONES PROACTIVAS Y MULTICAPA A OBJETO DE PREVENIR, SUBSANAR, CORREGIR Y PONER EN DERECHO A TODOS LOS COMPONENTES TECNOLÓGICOS DE LA INTRANET E INTERNET; HACIENDO CUMPLIR CON TODAS LAS DISPOSICIONES DE SEGURIDAD CORRELACIONADAS A LA LEY CIVIL Y PENAL.

### 5.1. Objetivos Específicos.

---

- **Identificar y Concentrar en una disposición normativa las obligaciones tecnológicas a las que la organización se enfrenta**, se requiere un repositorio de documentación legal o como marco normativo de control de todas las actividades identificadas para garantizar el cumplimiento de las obligaciones tecnológicas.
- **Establecer responsabilidades tecnológicas claras dentro de la organización** de manera que cada usuario (persona digital) encargada de llevar a cabo su actividad de control tenga claro el qué, cuándo y cómo debe llevar a cabo dichas actividades.
- **Establecer una supervisión continua de control**, a través de un algoritmo Informático de evaluación y de alertas que responda cuando existan indicios de incumplimiento de las actividades y/u obligaciones.
- **Optimizar y maximizar el uso de los recursos tecnológicos**, realizar controles de calidad a todos los recursos tecnológicos en el marco de las disposiciones contractuales.
- **Disponer de un registro (log) de actividad o huellas digitales**, requerir la correcta configuración de las pistas de auditoria para identificar potenciales incumplimientos de las actividades contractuales.
- **Elaborar Contratos especializados con los usuarios de las Tecnologías de la Información**, es decir, implementar Contratos Electrónicos que permitan realizar un control funcional acerca del cumplimiento de las obligaciones contractuales en favor de la entidad corporativa.

### 6. ALCANCE DE LA PROPUESTA.

---

La propuesta está configurada al desarrollo e implementación de 3 (tres) ejes temáticos acordes a las necesidades corporativas:

- **Dominio de Control PREVENTIVO – ASPECTOS LEGALES Y DEBIDO PROCESO EN TI. – TECNOLOGÍAS LEGALES INTELIGENTES.**  
«SI LA INSEGURIDAD DE LA INFORMACIÓN ES LA CONSTANTE NEGATIVA DENTRO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN, ENTONCES, LAS TECNOLOGÍAS INTELIGENTES Y LA INFORMÁTICA FORENSE SERÍA LA CONTRAPARTE INVERSA PARA RESOLVER Y MITIGAR LAS VULNERABILIDADES, RIESGOS E INCIDENTES LEGALES EN TI»
- **Dominio de Control CORRECTIVO - INFORMÁTICA FORENSE Y ANÁLISIS E INTERPRETACIÓN DE LA EVIDENCIA DIGITAL.**  
«TÉCNICA METODOLÓGICA QUE GARANTIZA LA AVERIGUACIÓN DE LA VERDAD, MEDIANTE LA CONSTRUCCIÓN DE UN MODELO MATEMÁTICO Y/O ALGORITMOS ABIERTOS Y AUDITABLES QUE PERMITEN EL CORRECTO ANÁLISIS E INTERPRETACIÓN DE LA EVIDENCIA DIGITAL. CONTRARIAMENTE, EL ANÁLISIS E INTERPRETACIÓN DE LA EVIDENCIA DIGITAL NO TENDRÍA NINGÚN SENTIDO»
- **Dominio de Control CONFORMIDAD Y SOPORTE LEGAL.**

«QUIEN TIENE EL CONOCIMIENTO SOBRE EL CONOCIMIENTO, TIENE EL PODER»

### Producto Global.

#### «ASEGURAMIENTO AL 100% DE LAS TECNOLOGÍAS DE LA INFORMACIÓN»

- Regular, Reglamentar y Fiscalizar la conducta humana de la persona digital (usuario) a objeto de minimizar y mitigar las Vulnerabilidades, Riesgos e Incidentes en el entorno Legal de las Tecnologías de la Información;
- Minimizar los riesgos legales en Delitos Informáticos, Ilícitos Informáticos, Contratos lesivos en TI, Afectación a la Billetera Digital, Pérdida patrimonial, Empleados deshonestos, Robo de información, Mail anónimos y agresivos, Extorsiones y Suplantación de Identidad, Espionaje Tecnológico, Fraude Corporativo, Pornografía, Libertinaje Digital, Acoso Sexual, entre otros.
- Reduce costos y riesgos, aumenta la eficacia y eficiencia de los Recursos Humanos.
- Proporciona un máximo retorno de la inversión.
- Contribuye a garantizar la satisfacción de los clientes y usuarios.
- Aseguramiento al 100% de las Tecnologías de la Información.

## 7. MATRIZ DE CONSISTENCIA DE LA PROPUESTA.

| PROBLEMA                                                                                                                                                                                                                                                                                                                                                                                    | OBJETIVO                                                                                                                                                                                                                                                                                                                         | HIPÓTESIS                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- Inexistencia de una Ley (Informática) coercitiva y actualizada.</li> <li>- Vertiginoso crecimiento de las TI vs Leyes y Normas estáticas y burocráticas.</li> <li>- Sistemas Informáticos: débiles, inseguros, excesivamente onerosos.</li> <li>- Recurrente problemas, caos, inseguridad, desconfianza en la administración de las TI.</li> </ul> | <p>Implementar las Tecnologías Legales Inteligentes, mediante la construcción de una norma o Ley Informática Inteligente a objeto de garantizar la Seguridad y Confiabilidad de las Tecnologías de la Información al 100%, haciendo cumplir con todas las disposiciones de Seguridad correlacionadas a la ley Civil y Penal.</p> | <p>Con la Implementación de las Tecnologías Legales Inteligentes se minimizará cualquier indicio de fraude tecnológico, se recuperará la potencial fuga de recursos económicos en la Billetera Digital y Patrimonio Tecnológico, se reducirán costos y riesgos operativos y mejorará la satisfacción e imagen corporativa.</p> |
| PROVOCA                                                                                                                                                                                                                                                                                                                                                                                     | PARA                                                                                                                                                                                                                                                                                                                             | PERMITIRÁ                                                                                                                                                                                                                                                                                                                      |
| <ul style="list-style-type: none"> <li>- Libertinaje Digital.</li> <li>- Afectación al Patrimonio y Billetera Digital.</li> <li>- Continuas y onerosas inversiones en TI.</li> <li>- Actividades delincuenciales por medios tecnológicos.</li> <li>- Diversas susceptibilidades en la gerencia ante la débil estructura de Seguridad Jurídica y Tecnológica.</li> </ul>                     | <ul style="list-style-type: none"> <li>- Erradicar cualquier nivel de corrupción en la manipulación del dato, proceso e información por parte de los usuarios.</li> <li>- Minimizar los Riesgos, Vulnerabilidades e Incidentes Legales en el entorno de las Tecnologías de la Información.</li> </ul>                            | <ul style="list-style-type: none"> <li>- Garantizar al 100% la seguridad y confiabilidad en el entorno de las TI.</li> <li>- Incrementar los beneficios económicos y patrimoniales.</li> </ul>                                                                                                                                 |

## 8. IMPACTO ESPERADO.

- Tecnologías de la Información con alto porcentaje de confiabilidad;

- Tecnologías de la Información alineadas a la ley Civil y Penal;
- Tecnologías de la Información debidamente configuradas;
- Protección integral técnico/legal de la “billetera digital” y del patrimonio tecnológico;
- Aprovechamiento positivo de los recursos tecnológicos;
- Control de actividades y obligaciones contractuales en Tecnologías de la Información;
- Incremento de productividad en todas las áreas;
- Disminución de vulnerabilidades y riesgos;
- Recuperación de inversiones tecnológicas;
- Incremento de credibilidad en la imagen corporativa, entre otros impactos.

## **9. CRONOGRAMA Y PROGRAMACIÓN DE ACTIVIDADES.**

---

La propuesta será desarrollada en 3 (tres) fases:

- Fase 1. Proceso de Diagnóstico con una duración de 1 a 4 semanas calendario;
- Fase 2. Proceso de Ejecución con una duración de 1 a 12 semanas calendario.
- Fase 3. Proceso de Capacitación, 40 horas académicas.

El cronograma propuesto podrá variar de acuerdo a las características de la organización.

## **10. PERSONAL ACREDITADO.**

---

### **Dirección Ejecutiva.**

- Especializado en Informática y Derecho.
- Personal acreditado en Informática, Ing. de Sistemas, Ing. en Telecomunicaciones y Redes Telemáticas, Derecho con experiencia en Gobierno y Comercio Electrónico, Firma Digital, Certificación Electrónica, Civil y Penal.

## **11. COSTO DE LA OFERTA.**

---

El costo puede variar en base a la dimensión tecnológica y será determinado entre partes.

## **12. FORMA DE PAGO.**

---

- 10% a la firma del Contrato;
- 30% contra entrega del informe del Proceso de Diagnóstico – Fase 1;
- 30% contra entrega del Informe del Proceso de Ejecución – Fase 2;
- 30% contra entrega del Informe del Proceso de Capacitación – Fase 3.

## **13. CONTINUIDAD DEL SOPORTE DE IT-LEGAL.**

---

La presente propuesta es auto sostenible por el lapso de 2 años o hasta que sea modificada la estructura normativa en Tecnologías de la Información; sin embargo, nuestros servicios podrán ser continuados en la Asistencia y Asesoramiento en IT-Legal

de acuerdo a las necesidades de su organización por un costo mensual que será determinado entre partes.

**Restricciones.**

- Todo tipo de comunicaciones y/o peticiones que suponga un acto delictivo o ilegal.
- Asistencia y Asesoramiento en IT-Legal para la construcción de herramientas tecnológicas que permitan actos delictivos.
- Soporte a problemas eminentemente técnicos.

**Confidencialidad y Privacidad.**

El Asesor Legal garantiza y compromete la más absoluta reserva, confidencialidad y privacidad en el resguardo de los datos o información proporcionada por el cliente.