«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)

Código de práctica para el aseguramiento eficiente y eficaz de las Tecnologías de la Información mediante la construcción de lineamientos técnico/legales a objeto de:

«Minimizar y mitigar las Vulnerabilidades, Riesgos e Incidentes Legales en el entorno de las TIC, mediante la implementación y construcción de soluciones proactivas y multicapa para 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», garantizando la Seguridad de las Tecnologías de la Información al 100%

Incluye el Código de práctica procedimental para la investigación de Delitos Informáticos:

- Informática Forense e Ingeniería Jurídica en los Delitos Informáticos;
- Análisis e Interpretación de la Evidencia Digital.

Information Technology Legal (IT-Legal)
Code of practice for information legal security management.

Este producto está sometido a la discusión pública; sin embargo, puede ser utilizado como base para implementar estándares configurados a los Aspectos Legales en Seguridad a fin de minimizar las vulnerabilidades, riesgos y resolver los incidentes legales en Tecnologías de la Información.

Las observaciones pueden ser sometidas y remitidas a:

Email: ejeguino@gmail.com

WhatsApp: +591 70617170 +591 70628589

Dirección: Calle José María Zalles Nº 923, San Miguel, zona Sur de la ciudad de La Paz

PREFACIO

EL PRESENTE CÓDIGO DE PRÁCTICA HA SIDO DESARROLLADO ANTE LA NECESIDAD DE MAXIMIZAR, SOCIALIZAR E IMPLEMENTAR ACCIONES OPORTUNAS, EFICIENTES Y EFICACES ACERCA DEL CONOCIMIENTO TEÓRICO, PRÁCTICO Y CIENTÍFICO DEL DERECHO VINCULADO A LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN.

EN ESTE CÓDIGO, SE TRATA DE INTRODUCIR Y RELACIONAR ESTUDIOS ACADÉMICOS, CIENTÍFICOS, EXPERIMENTALES Y EMPÍRICOS PARA ESTABLECER LOS MECANISMOS LEGALES MÁS IDÓNEOS PARA MINIMIZAR LAS VULNERABILIDADES Y RIESGOS LEGALES EN EL ENTORNO DE LAS TIC; ADICIONALMENTE, NOS PERMITE INTRODUCIR FORMATOS Y TÉCNICAS PARA RESOLVER LOS INCIDENTES LEGALES EN TIC, QUE GENERALMENTE, DERIVAN EN "DELITOS INFORMÁTICOS" O ACCIONES ANTIJURÍDICAS VINCULADAS CON LAS TIC QUE NO ESTÁN TIPIFICADAS EN LA LEGISLACIÓN PENAL Y QUE ESTÁN CAUSANDO DIVERSOS EFECTOS JURÍDICOS A NIVEL CORPORATIVO Y A NIVEL PERSONAL.

LA VISIÓN PROPOSITIVA DE ESTE CÓDIGO DE PRÁCTICA, ES APORTAR CON INSTRUMENTOS LEGALES PARA CONTRARRESTAR Y MINIMIZAR LAS VULNERABILIDADES, RIESGOS E INCIDENTES LEGALES EN TIC QUE CADA DÍA SE HACEN MÁS INIMAGINABLES EN SU DIMENSIÓN TECNOLÓGICA AL INTRODUCIRSE CONSTANTEMENTE NUEVAS FORMAS DE DELINQUIR Y ACRECENTAR LA "INSEGURIDAD EN TIC", Y QUE SON PARTE DE LOS DIVERSOS DEBATES Y REFLEXIONES SOBRE LA CIBERDELINCUENCIA A CONSECUENCIA DE LOS VACÍOS JURÍDICOS EN LAS DIFERENTES LEGISLACIONES A NIVEL MUNDIAL, EN ESPECIAL, SOBRE LO VENIDERO EN LA INTELIGENCIA ARTIFICIAL (IA), ROBÓTICA, PLATAFORMA CUÁNTICA, NANOTECNOLOGÍA Y OTRAS NOVEDOSAS CAPACIDADES TECNOLÓGICAS.

NO CABE DUDA, QUE LOS ÍNDICES DELINCUENCIALES EN TIC, ESTÁN ALCANZANDO NIVELES DE ALTA PREOCUPACIÓN POR LAS DIVERSAS CARACTERÍSTICAS DE LA CIBERDELINCUENCIA QUE ESTÁN RELACIONADOS CON EL CIBERESPACIO (NO EXISTEN FRONTERAS), PERSONA DIGITAL (LAS PERSONAS PUEDEN OCULTAR SU IDENTIDAD), LIBERTINAJE DIGITAL, INEXISTENCIA DE LEGISLACIÓN ESPECIALIZADA EN TIC, INEXISTENCIA DE RECURSOS HUMANOS ESPECIALIZADOS EN LA INVESTIGACIÓN DE LOS DELITOS INFORMÁTICOS, ENTRE OTROS.

POR OTRO LADO, EL CRECIMIENTO VERTIGINOSO DE LAS TIC ESTÁ PERMITIENDO GENERAR UNA CONTINUA Y NOVEDOSA FORMA DE INTERACTUAR ENTRE LAS PERSONAS (PERSONA DIGITAL) CON LOS RECURSOS TECNOLÓGICOS (REDES SOCIALES) A TRAVÉS DE UN TELÉFONO INTELIGENTE (SMARTPHONE) O UN COMPUTADOR U OTRO MEDIO ANÁLOGO, PRODUCIENDO EN ELLO, CAMBIOS ESTRUCTURALES EN EL COMPORTAMIENTO DEL SER HUMANO; ES MÁS, DIVERSAS INSTITUCIONES PÚBLICAS Y PRIVADAS OTORGAN MAYOR PERMISIBILIDAD (LIBERTINAJE DIGITAL) A LAS PERSONAS PARA CORRELACIONARSE CON EL MERCADO DIGITAL, ESTANDO CADA VEZ MÁS COMPROMETIDO CON LAS ESFERAS DEL ÁMBITO TECNOLÓGICO, REALIZANDO SUS PRINCIPALES ACTIVIDADES SOCIALES, LABORALES, COMERCIALES, ECONÓMICAS, FINANCIERAS Y COGNOSCITIVAS EN EL ENTORNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN.

EL AUTOR.

REGLAS GENERALES.

Este material ha sido desarrollado con una visión científica a objeto de minimizar los niveles de Vulnerabilidad, Riesgos e Incidentes Legales en el entorno de las TIC; para ello, se utilizarán algunos conceptos que serán muy útiles para su interpretación:

CIENCIA, TECNOLOGÍA E INVESTIGACIÓN	- **DESARROLLADA EN TAN SÓLO ALGUNOS AÑOS EN BENEFICIO (EN SENTIDO POSITIVO) Y EN CONTRA (EN SENTIDO NEGATIVO) DE LA SOCIEDAD EN GENERAL.**
	- **PROCESO DE CRECIMIENTO CONTINUO Y DESCONTROLADO.**
	- **SOLO PUEDE SER COMPRENDIDA Y DESARROLLADA POR UNA MENTE HUMANA; SIN EMBARGO, SE AVECINAN CAMBIOS ESTRUCTURALES CON LA NANOTECNOLOGÍA, ROBÓTICA, COMPUTACIÓN CUÁNTICA, INTELIGENCIA ARTIFICIAL QUE SOLO PODRÁ SER COMPRENDIDA Y DESARROLLADA POR ENTES TECNOLÓGICOS.**
	- **PRINCIPIO UNIVERSAL PARA EL CONSUMO HUMANO.**
	- **PATRIMONIO DE LA HUMANIDAD QUE SE DEBE PROTEGER, DESARROLLAR Y SOCIALIZAR EN EL CONOCIMIENTO HUMANO.**
	- **EN SENTIDO NEGATIVO, HA SIDO DESARROLLADA POR AGENTES PATÓGENOS DE LAS TIC, CON LA FINALIDAD DE EXPLOTAR LOS DIVERSOS NIVELES DE LA CIBERDELINCUENCIA:** CONTRATOS LESIVOS EN TIC; 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.

En este Código de Práctica, están expuestos de manera bastante asequible los resultados de la investigación científica y tecnológica a través de la construcción de modelos matemáticos correlacionados entre el Derecho con la Ciencia, Tecnología e Investigación y ésa será, la regla general para el proceso del aseguramiento legal de las Tecnologías de la Información:

IF, THEN, ELSE

Si pasa "X", entonces ocurrirá "Y"

Si NO pasa "X", entonces nunca ocurrirá "Y"

Este Código de Práctica en seguridad (legal) de las TIC es una guía desarrollada para todas aquellas personas naturales y jurídicas interesadas en el aseguramiento integral de las Tecnologías de la Información; desarrollada y enfocada para personas aficionadas a la Ciencia, Tecnología e Investigación, incluso para aquellas personas que son vagamente conscientes de que la Seguridad es importante y podría ser interesante para quienes aprecian los detalles técnicos; pero mucho más importante, para aquellas personas que son propietarios de la Información.

«La Información es Poder»

«Quién tiene la Información, tiene el Poder»

«Quién tiene el Conocimiento sobre el Conocimiento, tiene el Poder»

En los últimos años, se han producido profundas modificaciones en el escenario tecnológico mundial, así como un insostenible crecimiento de las TIC; crecimiento impar con la evolución legislativa en TIC y peor aún, ante la inexistencia de instrumentos legales en Seguridad de las Tecnologías de la Información, lo cual es motivante para el crecimiento de la ciberdelincuencia, debe entenderse, que constantemente aparecen nuevas formas de delinquir.

«Profundiza tu conocimiento en base a la producción de la Ciencia, Tecnología e Investigación»

Este insostenible crecimiento de las TIC, profundiza la “brecha digital” entre las grandes transnacionales productoras de tecnología con las regiones subdesarrolladas, que experimentan una gravísima degradación tecnológica producto de la imposición del conocimiento; promoviendo (de alguna forma), al uso y explotación tecnológica de los recursos tecnológicos foráneos que tienen el control (espionaje) digital en las diversas esferas políticas de Estado, industriales, comerciales, financieras, patrimoniales, entre otras.

«No existe el Crimen (cybercrimen) perfecto; sino, la investigación imperfecta»

Paradójicamente, el cybercrimen o ciberdelincuencia se parece cada vez a una ciencia por las características de la misma y la complejidad de su investigación.

«Los resultados de la Informática Forense no son casuales o fortuitos, son el resultado de la aplicación de un modelo matemático correlacionado con el derecho (informático)»

Este Código de Práctica, puede ser una sinopsis de la literatura científica que nos permita contraponer los objetivos tecnológicos del cybercrimen

EL AUTOR.

CONTENIDO

TECNOLOGIAS LEGALES INTELIGENTES

LEY INFORMÁTICA INTELIGENTE

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)

Código de práctica para la administración e implementación de recursos legales en el entorno legal de las Tecnologías de la Información.

Por lo general, los responsables del área de Tecnologías de la Información en las diversas organizaciones limitan el alcance de la "seguridad" a la configuración del firewall, robustez de la contraseña, actualización del antivirus, antispam, antimalware, antiramsonware y cualquier anti… que "supuestamente" proteja los recursos tecnológicos.

Estos diversos antis… tan sólo hacen lo que deben hacer, no hacen nada más… en consecuencia, no son suficientes para la protección integral de las Tecnologías de la Información; por el contrario, resultan ser productos intromisivos que pueden recorrer todos los espacios digitales de la Intranet e Internet. ¡ESO RESULTA SER MÁS PELIGROSO!!!

El Diseño, Operación, Uso y Administración de las Tecnologías de la Información deben estar sujetos a requisitos de Seguridad Legal, Normativa y Contractual.

OBJETIVO GENERAL:

Asegurar al 100% las Tecnologías de la Información, a través de la implementación y construcción de soluciones proactivas y multicapa para 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.

RESULTADOS ESPERADOS:

- Desarrollar una Ley "inteligente" que permita evolucionar al mismo ritmo que evoluciona 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;

- Recursos Tecnológicos al 100% de confiabilidad y garantiza su uso adecuado;

- Minimizar los riesgos legales en Delitos Informáticos, Ilícitos Informáticos, Contratos lesivos en Tecnologías de la Información, 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.

- Reducir costos y riesgos operativos en la administración de Tecnologías de la Información;

- Minimizará potenciales actos de sabotaje contra la organización;

- Aumenta la eficacia y eficiencia empresarial.

- Proporciona un máximo retorno de la inversión.

- Contribuye a garantizar la satisfacción de los clientes.

MATRIZ DE CONSISTENCIA:

PROBLEMA	OBJETIVO	HIPÓTESIS
- Inexistencia de una Ley (Informática) coercitiva y actualizada. - Vertiginoso crecimiento de las TI vs Leyes y Normas estáticas y burocráticas. - Sistemas Informáticos: débiles, inseguros, excesivamente onerosos. - Recurrente problemas, caos, inseguridad, desconfianza en la administración de las TI.	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.	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.
PROVOCA	**PARA**	**PERMITIRÁ**
- Libertinaje Digital. - Afectación al Patrimonio y Billetera Digital. - Continuas y onerosas inversiones en TI. - Actividades delincuenciales por medios tecnológicos. - Diversas susceptibilidades en la gerencia ante la débil estructura de Seguridad Jurídica y Tecnológica.	- Erradicar cualquier nivel de corrupción en la manipulación del dato, proceso e información por parte de los usuarios. - Minimizar los Riesgos, Vulnerabilidades e Incidentes Legales en el entorno de las Tecnologías de la Información.	- Garantizar al 100% la seguridad y confiabilidad en el entorno de las TI. - Incrementar los beneficios económicos y patrimoniales.