UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA

Tendencias Tecnológicas

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Profesor: Lic. César Augusto Angulo Calderón

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

La seguridad electrónica creció un 250% en los últimos 10 años en nuestro país. Hoy emplea a más de 14.500 personas y factura u$s 755 millones al año.

En la década del 80 hablábamos sólo de alarmas sonoras y sistemas básicos de detección de incendios. Treinta años después contamos con tecnologías para reconocer en vivo rostros en la oscuridad a través de cámaras de visión nocturna automatizadas.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

La tecnología evolucionó, el mercado creció, los delitos se complejizaron y los riesgos aumentaron pero el sector de la seguridad electrónica sigue sin tener una legislación nacional que lo regule.

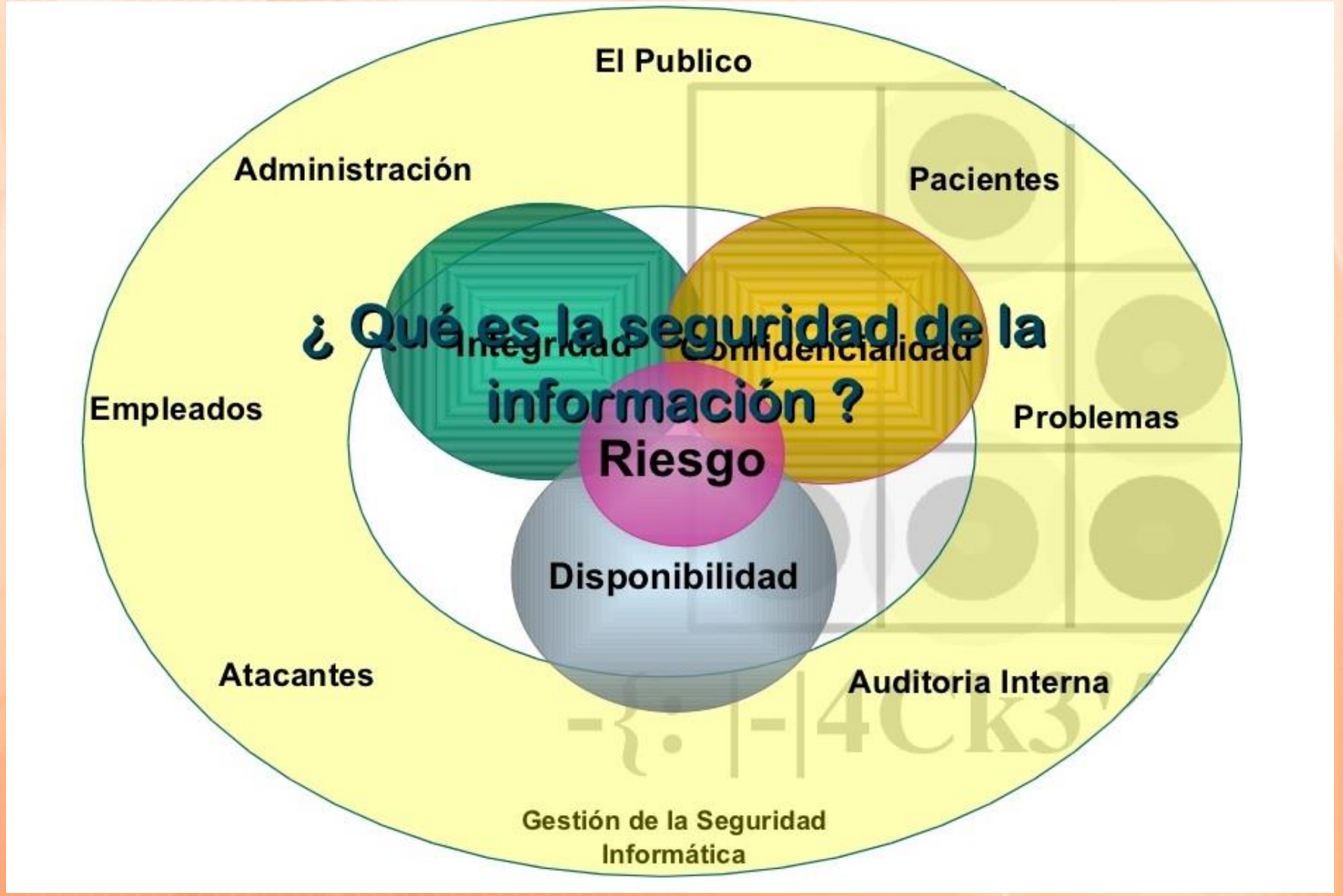
Hasta el día del hoy se maneja con un conjunto de leyes parciales, normas y disposiciones atrasadas e incompletas a nivel técnico y que desconocen la envergadura y particularidades de la seguridad electrónica poniendo en riesgo la viabilidad económica de las empresas y la seguridad en general.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

Técnicamente es imposible lograr un sistema informático ciento por ciento seguro, pero buenas medidas de seguridad evitan daños y problemas que pueden ocasionar intrusos.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN



SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

La seguridad de la información protege la información de una amplia gama de amenazas con el fin de asegurar la continuidad del negocio, minimizar el daño del negocio y maximizar el retorno de la inversión y las oportunidades de negocio.

Técnicamente es imposible lograr un sistema informático ciento por ciento seguro, pero buenas medidas de seguridad evitan daños y problemas que pueden ocasionar intrusos.

Riesgos, Amenazas y Vulnerabilidades

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

¿Qué se debe asegurar?

Nuevos escenarios:

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

¿Qué se debe asegurar?

La información debe considerarse como un recurso con el que cuentan las Organizaciones y por lo tanto tiene valor para éstas, al igual que el resto de los activos, debe estar debidamente protegida.

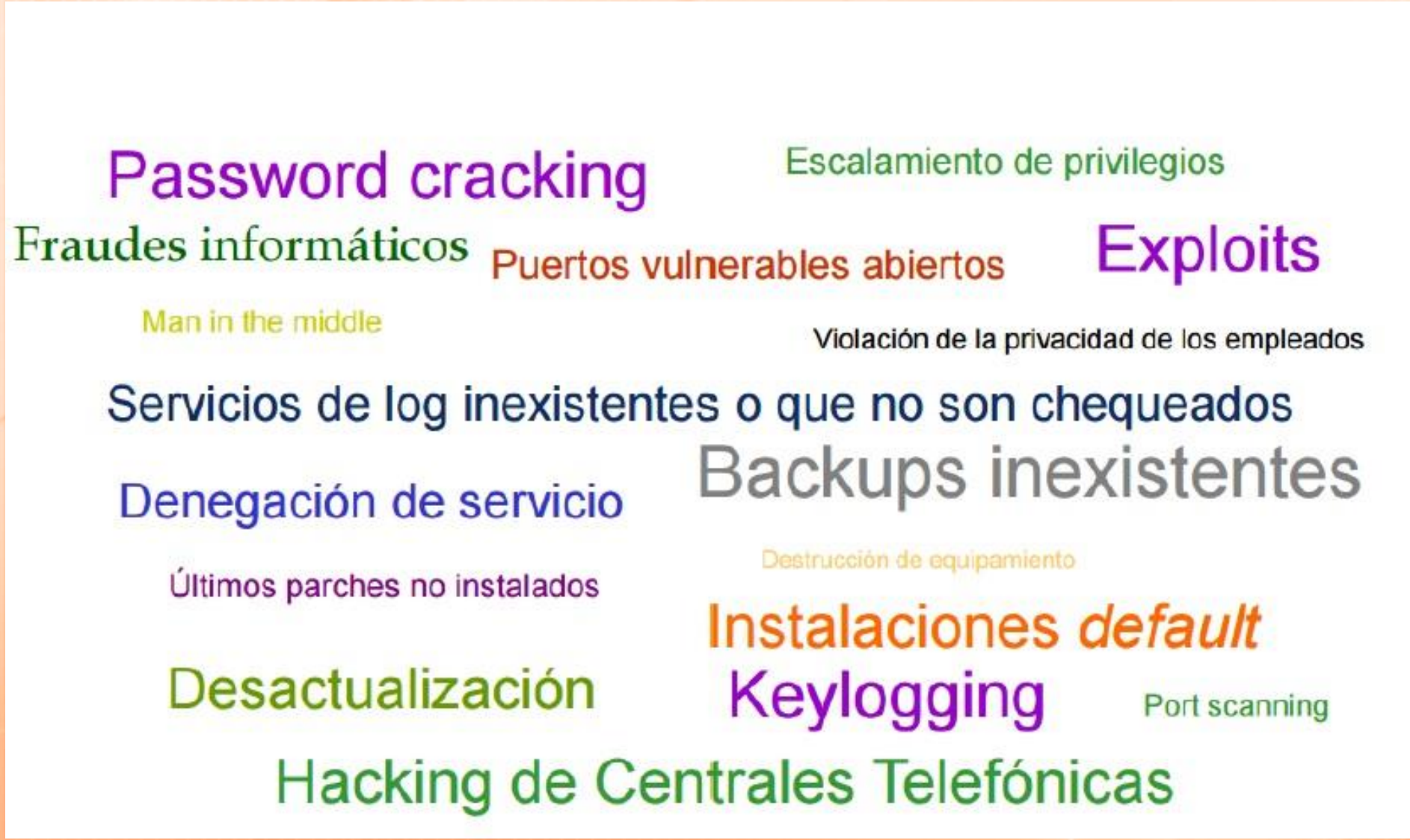
SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Amenaza

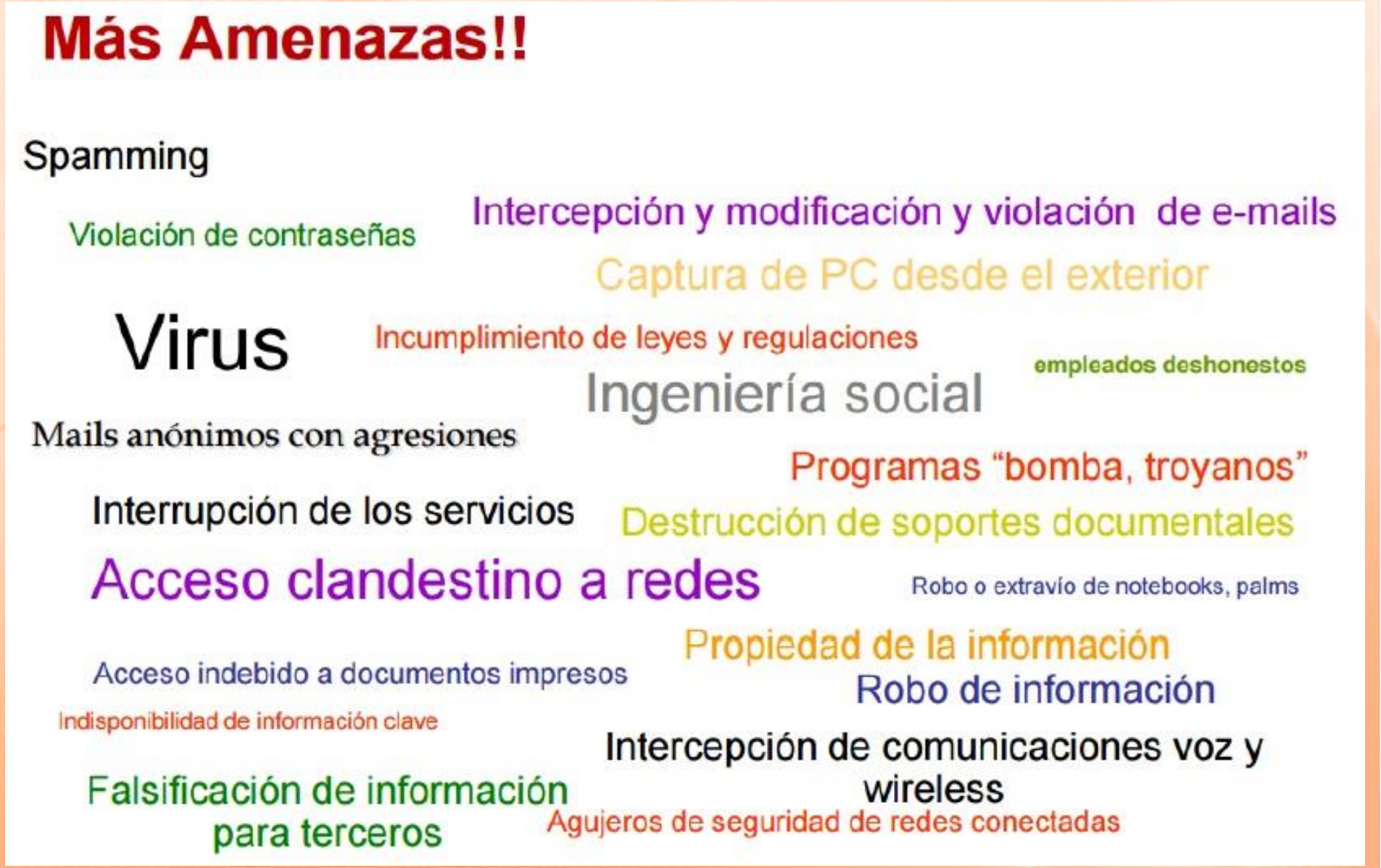
La amenaza puede definirse como aquel peligro latente, originado por un hecho o acontecimiento que aún no ha sucedido, o provocado por un evento natural o antropogénico (se refiere a los efectos, procesos o materiales que son el resultado de actividades humanas, a diferencia de los que tienen causas naturales sin influencia humana).

Diferentes tipo de amenazas

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN



SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN



SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Por qué aumentan las amenazas ?

- Crecimiento exponencial de las Redes y Usuarios Interconectados - Dependencia.
- Profusión de las BD On-Line
- Inmadurez de las Nuevas Tecnologías
- Alta disponibilidad de Herramientas Automatizadas de Ataques
- Nuevas Técnicas de Ataque Distribuido (Ej:DDoS)
- Técnicas de Ingeniería Social

Ataque Distribuido de Negación de Servicio (DDoS - Distributed Denial of Service)

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Cuáles son las amenazas?

Accidentes: Averías, Catástrofes, Interrupciones, ...

Errores: de Uso, Diseño, Control, ...

Intencionales Presenciales: Atentado con acceso físico no autorizado.

Intencionales Remotas: Requieren acceso al canal de comunicación.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Amenazas Intencionales Remotas

- Interceptación pasiva de la información (amenaza a la CONFIDENCIALIDAD).

- Corrupción o destrucción de la información (amenaza a la INTEGRIDAD).

- Suplantación de origen (amenaza a la AUTENTICACIÓN).

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Vulnerabilidad

Capacidad disminuida de una persona o un grupo de personas para anticiparse, hacer frente y resistir a los efectos de un peligro natural o causado por la actividad humana, y para recuperarse de los mismos.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Vulnerabilidades

- Inadecuado compromiso de la dirección.
- Personal inadecuadamente capacitado y concientizado.
- Inadecuada asignación de responsabilidades.
- Ausencia de políticas/ procedimientos.
- Ausencia de controles
  - (físicos/lógicos)
  - (disuasivos/preventivos/detectivos/correctivos)
- Ausencia de reportes de incidentes y vulnerabilidades.
- Inadecuado seguimiento y monitoreo de los controles.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Contra qué se debe proteger la Información ?

La Seguridad de la Información, protege a ésta de una amplia gama de amenazas, tanto de orden fortuito como destrucción, incendio o inundaciones, como de orden deliberado, tal como fraude, espionaje, sabotaje, vandalismo, etc.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Qué se debe garantizar ?

Confidencialidad: Se garantiza que la información es accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Se garantiza que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma toda vez que se requiera.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Las Organizaciones son cada vez mas dependientes de sus Sistemas y Servicios de Información, por lo tanto podemos afirmar que son cada vez mas vulnerables a las amenazas concernientes a su seguridad.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Riesgo

Es una medida de la magnitud de los daños frente a una situación peligrosa. El riesgo se mide asumiendo una determinada vulnerabilidad frente a cada tipo de peligro.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Amenazas, Riesgos & Vulnerabilidades

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Acciones de la ONGEI

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Actualmente la ONGEI apoya a las entidades públicas en los siguientes principales servicios:

- Análisis de vulnerabilidades de los servidores Web de las Entidades Publicas.
- Boletines de Seguridad de la información
- Boletines de Alertas de Antivirus.
- Presentaciones técnicas sobre seguridad.
- Consultorías y apoyo en recomendaciones técnicas.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Política de Seguridad para el Sector Público

Que se entiende por Política de Seguridad?

Conjunto de requisitos definidos por los responsables directos o indirectos de un Sistema que indica en términos generales qué está permitido y qué no lo está en el área de seguridad durante la operación general de dicho sistema.

Diferencias entre Política, Estándar y Procedimiento

Política: el porqué una organización protege la información.

Estándares: lo que la organización quiere hacer para implementar y administrar la seguridad de la información.

Procedimientos: cómo la organización obtendrá los requerimientos de seguridad

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

¿Cómo establecer los requerimientos de seguridad?

- **Evaluar los riesgos que enfrenta la organización**
  - Se identifican las amenazas a los activos
  - Se evalúan las vulnerabilidades y probabilidades de ocurrencia
  - Se estima el impacto potencial
- **Tener en cuenta los requisitos legales, normativos, reglamentarios y contractuales que deben cumplir:**
  - La organización
  - Sus socios comerciales
  - Los contratistas
  - Los prestadores de servicios
- **Establecer un conjunto específico de principios, objetivos y requisitos para el procesamiento de la información**

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

¿Qué se entiende por SGSI?

SGSI: Sistema de Gestión de la Seguridad de la Información
ISMS: Information Security Management System

Un modelo de gestión para la mejora continua de la calidad de la seguridad de la información.

- Realización de un análisis de riesgos
- Definición de una política de seguridad
- Establecimiento de controles

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

Con fecha 23 de julio del 2004 la PCM a través de la ONGEI, dispone el uso obligatorio de la **Norma Técnica Peruana "NTP – ISO/IEC 17799:2004 EDI.** Tecnología de la Información: Código de Buenas Prácticas para la Gestión de la Seguridad de la Información" en entidades del Sistema Nacional de Informática.

• Se Actualizó el 25 de Agosto del 2007 con la **Norma Técnica Peruana "NTP – ISO/IEC 17799:2007 EDI.**

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

- En este sentido La Norma Técnica Peruana ISO – 17799, se emite para ser considerada en la implementación de estrategias y planes de seguridad de la información de las Entidades Públicas.

- La NTP NO exige la certificación, pero si la consideración y evaluación de los principales dominios de acuerdo a la realidad de cada organización.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

¿Cuáles son los temas o dominios a considerar dentro de un plan de Seguridad?

Los 11 dominios de control de ISO 17799

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

1. **Política de seguridad:**
   Se necesita una política que refleje las expectativas de la organización en materia de seguridad, a fin de suministrar administración con dirección y soporte. La política también se puede utilizar como base para el estudio y evaluación
   en curso.

2. **Aspectos organizativos para la seguridad:**
   Sugiere diseñar una estructura de administración dentro la organización, que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

3. **Clasificación y Control de Activos:**
   Inventario de los recursos de información de la organización y con base en este conocimiento, debe asegurar que se brinde un nivel adecuado de protección.
4. **Seguridad de Recursos Humanos:**
   Necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. Implementa un plan para reportar los incidentes.
5. **Seguridad física y del Entorno:**
   Responde a la necesidad de proteger las áreas, el equipo y los controles generales.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

6. Gestión de Comunicaciones y Operaciones: Los objetivos de esta sección son:

- Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
- Minimizar el riesgo de falla de los sistemas.
- Proteger la integridad del software y la información.
- Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información.
- Garantizar la protección de la información en las redes y de la infraestructura de soporte.
- Evitar daños a los recursos de información e interrupciones en las actividades de la institución.
- Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

7. Control de accesos:

Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación como protección contra los abusos internos e intrusos externos.

8. Adquisición, Desarrollo y Mantenimiento de los sistemas:

Recuerda que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.

SEGURIDAD ELECTRÓNICA Y LEGISLACIÓN

9. Gestión de Incidentes de la Seguridad de la información

Asegurar que los eventos y debilidades en la seguridad de la información sean comunicados de manera que permitan una acción correctiva a tiempo.

10. Gestión de Continuidad del Negocio

Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la organización y para proteger los procesos importantes de la organización en caso de una falla grave o desastre.

11. Cumplimiento:

Evitar brechas de cualquier ley civil o criminal, estatutos, obligaciones regulatorias o contractuales y de cualquier requerimiento de seguridad.