Ciberseguridad

Viceministerio de Comunicaciones

Hacia un Perú Digital

Lima, agosto de 2017

Documento de trabajo para discusión interna, elaborado en el marco de las propuestas presentadas para el desarrollo de las TIC en el Perú

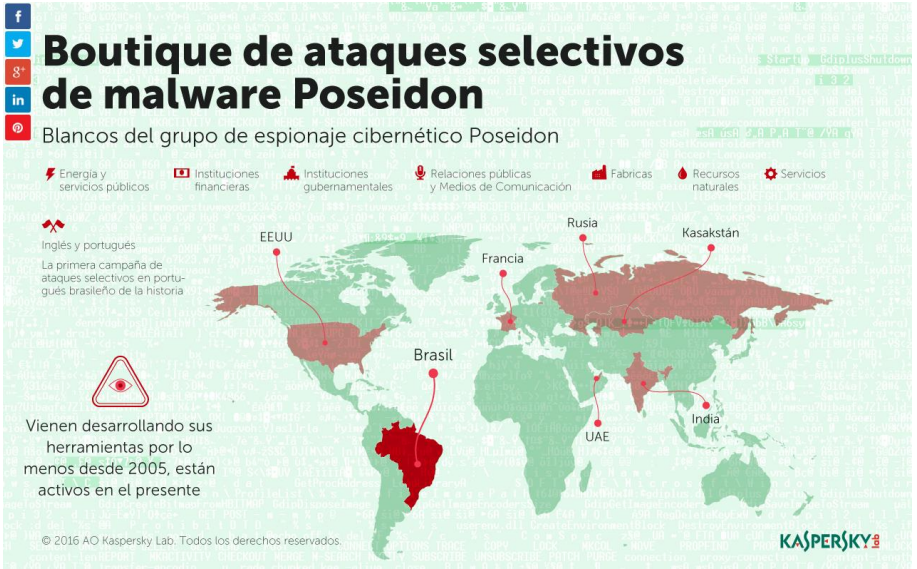
Objetivos

- Presentar la problemática de la ciberseguridad en el Perú
- Estrategias y propuestas que busca resolver esa problemática

Documento de trabajo para discusión interna, elaborado en el marco de las propuestas presentadas para el desarrollo de las TIC en el Perú

Riesgo de la transformación digital

- La transformación digital involucra una mayor penetración de la Internet y mejor interconexión de las personas
- Se incrementará el uso de nuevas tecnologías que usarán información vital para servicios críticos y sensibles
- Habrá un incremento del delito y abuso informático
- La ciberseguridad se convierte en un asunto clave y transversal a la sociedad de la información
- Ejemplos de ataques informáticos: Ransomware, ataques de denegación de servicios usando dispositivos IoT, robo de cuentas y datos personales por debilidades en las configuraciones, ataques y grupos organizados para el espionaje cibernético (Poseidon, Lazarous group, Hacking Team), phishing



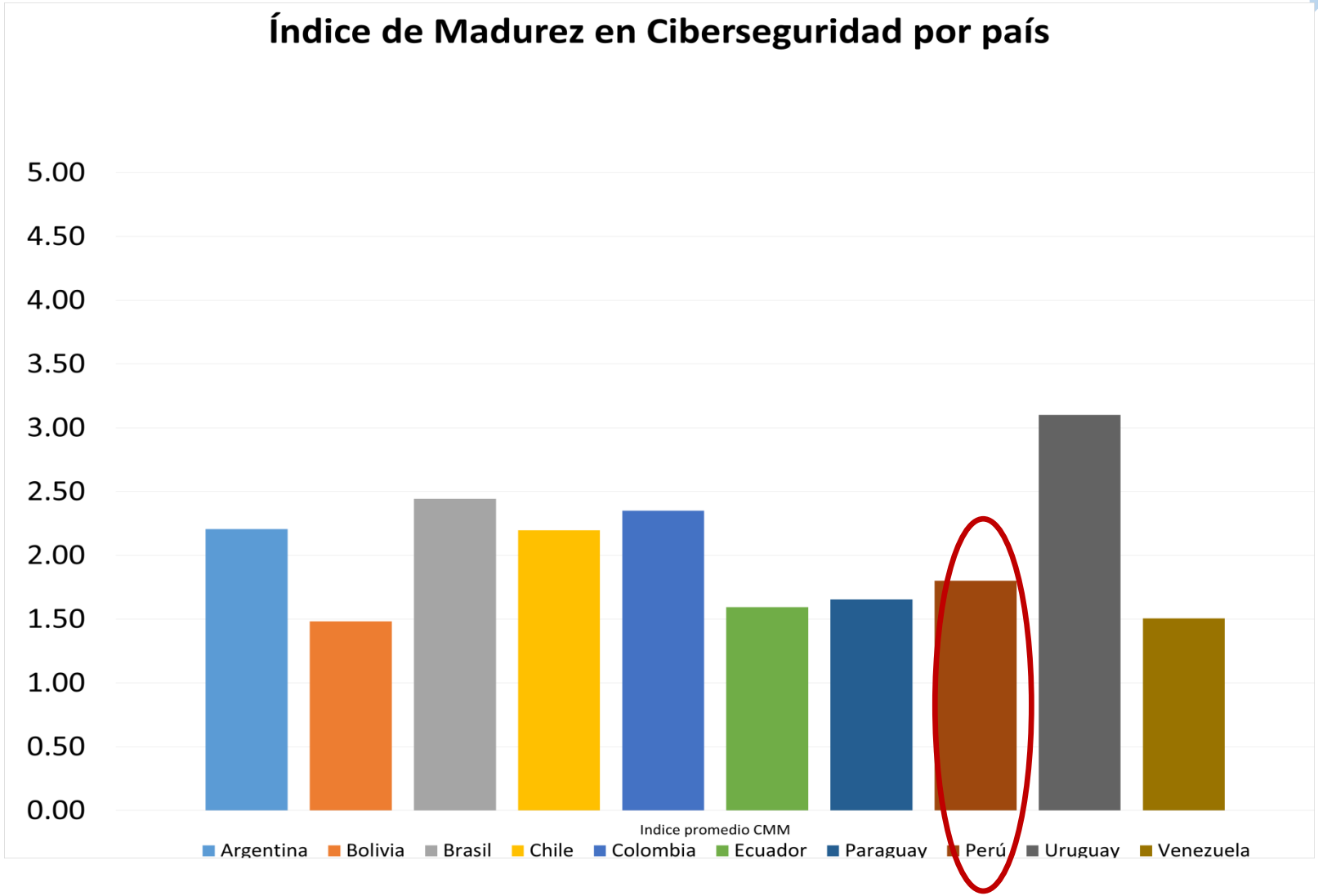
¿Cómo estamos en ciberseguridad?

- En el 2016 el BID hizo un informe sobre la ciberseguridad en Latinoamérica, basado en el modelo de madurez desarrollado por Centro Global de Capacidad sobre Seguridad Cibernética (Oxford) que utiliza 49 indicadores. Este estudio concluye que muchos países de la región son vulnerables a ataques cibernéticos potencialmente devastadores.
- Se han definido cinco niveles de madurez para los indicadores

Nivel		Descripción resumida
1	**Inicial**	Nada existe o es de naturaleza embrionaria
2	**Formativo**	Características nuevas, casuales, desorganizadas, mal definidas
3	**Establecido**	Elementos establecidos y funcionando, falta asignación de recursos
4	**Estratégico**	Se han elegido elementos que son clave, trabajando en función a resultados esperados
5	**Dinámico**	Mecanismos claros para adaptar la estrategia a las circunstancias imperantes. Toma de decisiones rápida.

¿Cómo estamos en ciberseguridad?

- Según el BID, en general, el promedio de los países sudamericanos es relativamente bajo
- El Perú llega a 1.8, superado por Uruguay, Argentina, Brasil, Chile y Colombia



¿Cómo estamos en ciberseguridad?

- En este año la UIT ha publicado el Índice de Ciberseguridad Global
- El índice tiene un mínimo de cero y un máximo de 1
- Según este indicador, Perú está en la posición 78 de 193 países, inclusive debajo de Ecuador

AMERICAS Region		
Country	**Score**	**Global Rank**
United States of America	0.919	2
Canada	0.818	9
Mexico	0.660	28
Uruguay	0.647	29
Brazil	0.593	38
Colombia	0.569	46
Panama	0.485	61
Argentina	0.482	62
Ecuador	0.466	65
Peru	0.374	78
Venezuela	0.372	79

Marco legal y situación actual

- Ley 27309 (jul-2000), Ley que incorpora los Delitos Informáticos al Código Penal.
- Ley 30096 (oct-2013), Ley de Delitos informáticos y su modificatoria la ley 30171
- RM 360-2009-PCM, que crea la Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú (Pe-CERT) Normativa de creación del PeCERT.
- *El ámbito de la PCERT no es suficiente (no incluye a toda la sociedad de la información).*
- En el marco normativo peruano no se encuentra un plan o estrategias nacionales de ciberseguridad

¿Qué podemos hacer? Algunos ejemplos

- Elaborar y documentar políticas y un plan de ciberseguridad alineados a los objetivos nacionales
- Desarrollar una gestión de la defensa cibernética con una estructura de mando clara
- Sensibilizar a la sociedad sobre las amenazas cibernéticas definiendo medidas concretas contra ellas
- Preparar instructores nacionales en ciberseguridad , dotar de un presupuesto para la educación e investigación en ese rubro
- Promover la divulgación responsable de la información de vulnerabilidades
- Aplicación de normas relacionas a ciberseguridad en los reglamentos de adquisiciones de equipos y software
- Implantar un centro de mando y control de ciberseguridad para los estamentos públicos y privados
- Planificar coordinadamente las respuestas a ataques a los activos críticos
- Desarrollar diálogos formales entre el sector público y privado para la protección de la infraestructura crítica nacional (ICN)
- Desarrollar conciencia de los operadores respecto a las amenazas a la ICN
- Promover la aplicación de la gestión de riesgos en las práctica empresariales para la protección de datos en todos los niveles
- Evaluar los protocolos y procedimientos para la gestión de crisis respecto a la ICN
- Planificar medidas de redundancia digital de la ICN
- Desarrollar un mercado de seguros contra la delincuencia cibernética

Documento de trabajo para discusión interna, elaborado en el marco de las propuestas presentadas para el desarrollo de Digital Identity

WEF – A Blueprint for a Digital Identity, Agosto 2016

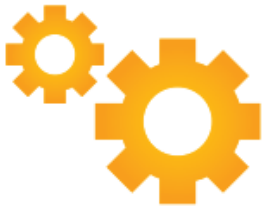
Ejemplos de políticas de ciberseguridad

El objetivo es impulsar un ecosistema digital confiable y seguro

- Establecer estándares para proteger la infraestructura crítica y datos sensibles
- Desarrollar y mantener grupos de expertos en seguridad informática, tanto en el sector privado como en el público
- Establecer un marco jurídico sólido para tipificar delitos y abuso informático
- Promover la educación y sensibilización del público con respecto a la ciberseguridad
- Desarrollar una cultura de ciberseguridad

Ámbito del Plan de Ciberseguridad

- Se debe establecer la competencia del plan coordinando con los todos los estamentos de la sociedad de la información
- El Plan debe contemplar políticas, objetivos y estrategias en los siguientes campos:



Medidas técnicas

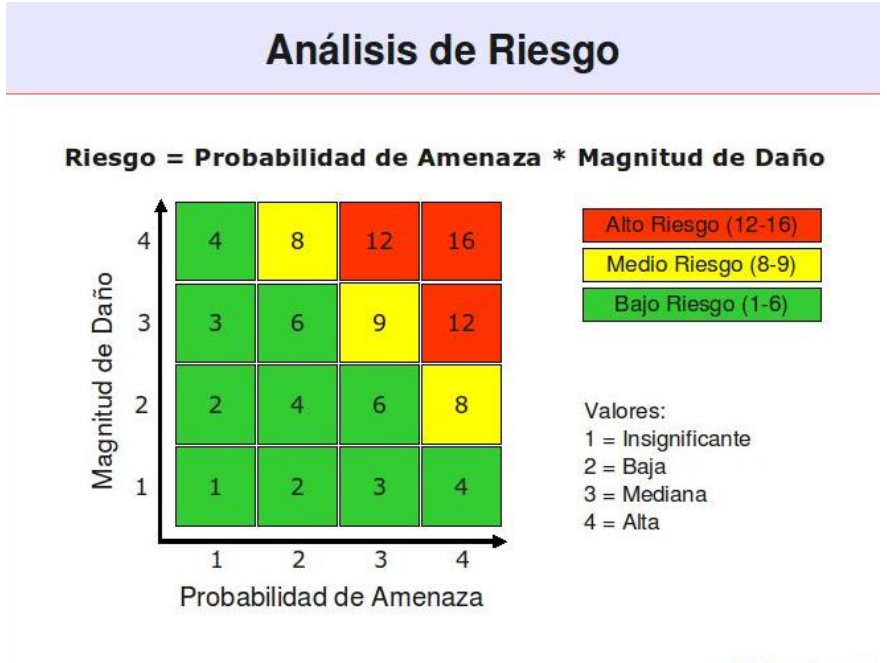
Recursos humanos
y desarrollo de capacidades

Legal y regulatorio

Educación
y conciencia pública

Algunas estrategias puntuales

- Trabajar en función a análisis de riesgos
- Estándares diferenciados para la implementación de la ciberseguridad, a fin de no afectar la facilidad de uso y la masificación de servicios TIC
- Priorizar lo realmente crítico
- Creación de grupos de trabajo
- Mantenimiento de equipos de respuestas rápidas a incidentes de ciberseguridad



Recomendaciones de expertos

- Ninguna nación por sí sola puede asegurar adecuadamente sus redes. La cooperación es esencial -> Convenio de Budapest
- Las estrategias de ciberseguridad nacional deben armonizarse con los valores y derechos fundamentales, tales como la privacidad, la libertad de expresión y el debido proceso
- La ciberseguridad debe basarse en los principios técnicos clave que han permitido la innovación en Internet, tales como la apertura, la universalidad y la interoperabilidad
- Cuando la ciberseguridad se centra exclusivamente en asuntos militares y de inteligencia, es posible que no alcancen un equilibrio adecuado entre la seguridad y los derechos, tales como la privacidad y la libertad de expresión y de asociación

Objetivo del Grupo de Trabajo

Grupo 1:

- Definir grado de importancia de los resultados que emita la Mesa de Ciberseguridad (aplicabilidad)
- Análisis situación de la Ciberseguridad del país, desarrollo de un árbol de problemas
- Identificar las agencias de gobierno que están directamente vinculadas a este tema

Objetivo del Grupo de Trabajo

Grupo 2:

- Sensibilizar y comunicar sobre Ciberseguridad
- Articular con las diferentes entidades tanto privadas, públicas y academia sobre Ciberseguridad
- Mapeo, línea base (presentación de PCM, para ver lo avanzado)
- Mejorar, plantear lineamientos, necesidades y propuestas

Pedir una presentación de la fuerza aérea)

Objetivo del Grupo de Trabajo

Grupo 3:

- Un diagnóstico de la seguridad en las entidades del estado.
- Campaña de sensibilización
- Coordinación o articulación en las direcciones de las diversas organizaciones
- Compartir las experiencias entre las entidades ante determinado evento (Gestión del Conocimiento), definir protocolo

Estructura del Grupo de Trabajo

Representantes privados:

- Academia: Inictel – UNI (José Luis Quiroz Arroyo)
- Sociedad Civil: Hiperderecho (Carlos Guerrero Argote)
- Gremios: Apesol (Damaso Fonseca Boy)

Representante público:

Secretaria de Gobierno Digital (SEGDI / PE-CERT)

Próxima reunión: Miércoles 13 de Setiembre (MTC)

GRACIAS

Ministerio de Transportes y Comunicaciones

Viceministerio de Comunicaciones

Preparado por: Iván Otárola
Revisado por: Alfredo Astudillo