Seguridad informática en Uruguay
Investigación

Ing. Eduardo Carozo Blumsztein, Mgt, Cis.
Gerente de Seguridad de la Información
ANTEL

Esta es la primera vez que se realiza un Encuesta Nacional de estas características en nuestro país y en primer lugar quiero agradecer a las personas que generosamente han participado en la construcción de la información de base contestando la encuesta.

El análisis presentado a continuación se desarrollo basado en una muestra seleccionada de personas que respondió a una encuesta de manera interactiva a través de una página web dispuesta a tal fin. Dada la limitación de tiempo y recursos disponibles se realizarán un conjunto de análisis básicos, con el propósito de ofrecer los aspectos más importantes de manera de orientar al lector sobre las tendencias identificadas en el estudio.

Estructura de la encuesta

Fue diseñado un cuestionario compuesto por aproximadamente 30 preguntas sobre los siguientes aspectos:

1. Demografía
2. Presupuestos
3. Fallas de seguridad
4. Herramientas y prácticas de seguridad
5. Políticas de seguridad

Demografía:

Esta sección identifica los sectores que participan, el tamaño de la organización en la que participa el responderte, la dependencia organizacional de la seguridad y los cargos de las personas que respondieron las preguntas.

Presupuestos

Se analiza si las organizaciones han destinado rubros para la seguridad informática. Permite revisar el tipo de tecnología en el que invierten y un estimado del monto de la inversión en seguridad informática.

Fallas de seguridad

Esta sección revisa los tipos de fallas de seguridad más frecuentes, como se detectan y a quién se notifican. Intenta identificar las causas por las cuales no se denuncian y si existe la conciencia sobre la evidencia digital en la atención de incidentes de seguridad informática.

Herramientas y prácticas de seguridad informática

En este segmento de la encuesta, el objetivo es identificar las prácticas de las empresas sobre la seguridad, los dispositivos o herramientas que con más frecuencia utilizan para el desarrollo de la infraestructura tecnológica y las estrategias que utilizan las organizaciones para enterarse de las fallas de seguridad.

Políticas de seguridad

Finalmente se busca indagar sobre la formalidad de las políticas de seguridad en la organización; los principales obstáculos para lograr una adecuada seguridad, las buenas prácticas o estándares que se utilizan.

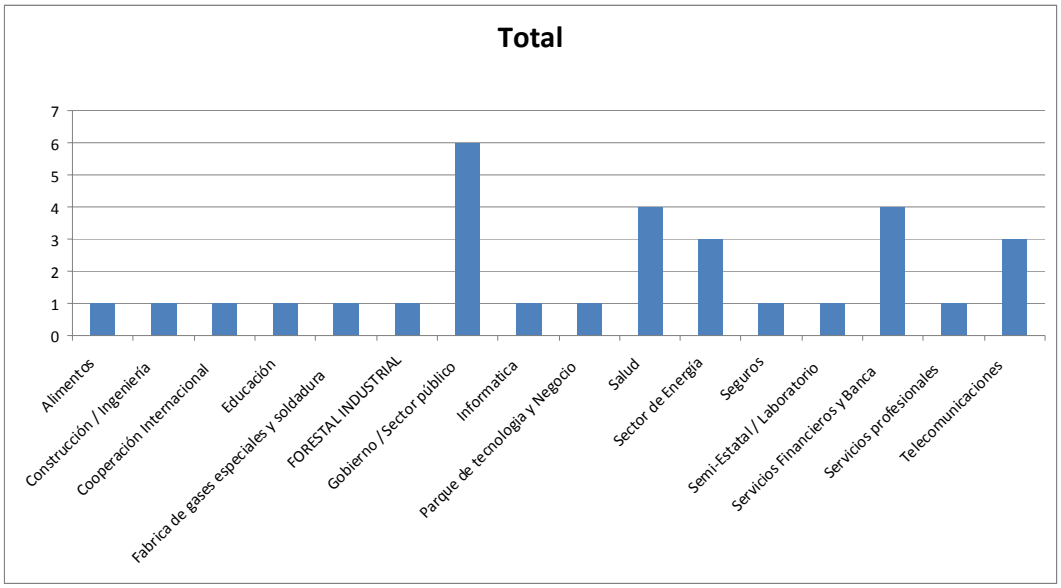
Consideraciones muestrales

Han participado de la muestra 31 personas que representan aproximadamente entre el 30% y el 40% de las personas con experiencia, que se dedican a éstas tareas en Uruguay, entendemos que si bien son pocos participantes para establecer un valor estadístico de confianza, el mismo se encuentra significativamente mejorado por la selección previa de las personas consultadas.
A continuación se presentan los resultados de la encuesta en porcentaje por temas y algunos comentarios relacionados con los datos obtenidos:

Demografía

Sectores participantes

¿A qué sector pertenece su compañía?	Total
Alimentos	3.2%
Construcción / Ingeniería	3.2%
Cooperación Internacional	3.2%
Educación	3.2%
Fabrica de gases especiales y soldadura	3.2%
FORESTAL INDUSTRIAL	3.2%
Gobierno / Sector público	19,4%
Informatica	3.2%
Parque de tecnologia y Negocio	3.2%
Salud	12.9%
Sector de Energía	9.6%
Seguros	3.2%
Semi-Estatal / Laboratorio	3.2%
Servicios Financieros y Banca	12.9%
Servicios profesionales	3.2%
Telecomunicaciones	9.6%
Total general	100%



Se observa predominancia del Gobierno/Sector Público, consecuencia de una estructura nacional muy particular de nuestro país, en el cual, la mayoría de las grandes compañías se encuentran en el estamento público.
Banca, Salud, Telecomunicaciones y Energía son los otros sectores más representados de acuerdo con la importancia de sus servicios para la comunidad.
En Uruguay nos encontramos con múltiples regulaciones en el sector Gobierno y Banca que están potenciando esta realidad y es de esperar que en el futuro estos sectores aumenten aún más su preocupación y la asignación de recursos a los aspectos de seguridad. En futuras ediciones de la misma podremos en la evolución, evaluar el impacto y la pertinencia de las regulaciones recientemente promulgadas.

Análisis del tamaño de las organizaciones (porcentaje)

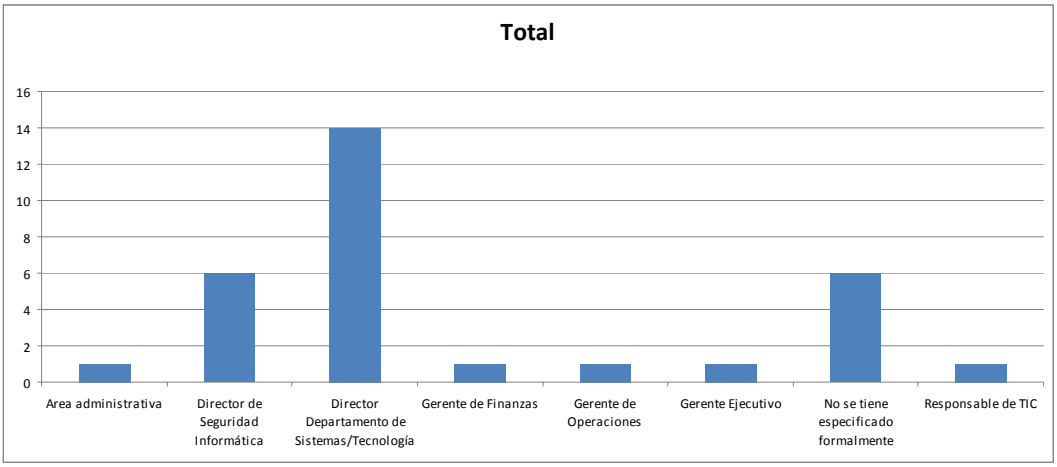
¿Cuántos empleados existen en total en su organización?	Total
1 a 50	3.2%
101 a 200	12.9%
201 a 300	9.7%
301 a 500	19.4%
501 a 1000	12.9%
51 a 100	6.5%
Más de 1000	35.5%
Total general	100%

Comentarios Generales:

Se han preseleccionado a personas con experiencia en el tema de seguridad lo que probablemente haya sesgado la encuesta hacia organizaciones de mediano a gran tamaño, esto se debe a que no existen formaciones de grado consolidadas en nuestro país, que puedan ser utilizadas como base de la muestra.

Dependencia organizacional del área de seguridad informática

¿De quién depende la responsabilidad de la seguridad informática de su organización?	Total
Área administrativa	3.2%
Director de Seguridad Informática	19.4%
Director Departamento de Sistemas/Tecnología	45.2%
Gerente de Finanzas	3.2%
Gerente de Operaciones	3.2%
Gerente Ejecutivo	3.2%
No se tiene especificado formalmente	19.4%
Responsable de TIC	3.2%
Total general	100%



Comentarios generales:

Los resultados muestran que existe un porcentaje relativamente alto de Directores de Seguridad Informática 19.4% en las empresas encuestadas. De todas formas aún se da en forma predominante una importante dependencia de Seguridad de la Información de las dependencias de Sistemas o Tecnologías de la Información.
Se espera que la aparición del CERT.uy a nivel del estado uruguayo propicie cambios significativos en el estado y eso por imitación sea adoptado por las empresas privadas principales.
Es significativo el alto número de casos en que aún no se tiene especificado formalmente el cargo del responsable de seguridad informática en la organización.

Cargos que respondieron la encuesta:

Su cargo en la organización es:	Total
Coordinador de Sistemas	3.2%
Director/Jefe de Seguridad Informática	9.7%
Gerente Operaciones	3.2%
IS Country Coordinator	3.2%
Operario	3.2%
Presidente/Gerente General	3.2%
Profesional de Departamento de Sistemas/Tecnología	52%
Profesional del Departamento de Seguridad Informática	9.7%
Profesor Agregado	3.2%
Responsable de Seguridad Informática	3.2%
Responsable de TIC	3.2%
Seguridad en Sistemas de Información	3.2%
Total general	100%

Es claro reconocer que la seguridad informática se encuentra mayoritariamente dependiente de tecnologías de la información en Uruguay. La aparición reciente de los Directores/Gerentes de Seguridad muestra que de a poco se va reconociendo la importancia de este tema en la Dirección de las Organizaciones.
Se visualiza de todas formas que el tema es importante para la alta gerencia, siempre dentro del contexto del negocio.

Presupuesto

El presupuesto global de informática de su organización, incluye aspectos de seguridad de la información?	Total
En Blanco	16.1%
No	25.8%
Si	58.1%
Total general	100%

Comentarios Generales

Como se puede ver alrededor del 60% de las organizaciones nacionales han declarado tener un presupuesto dedicado a Seguridad Informática. Esta situación no se corresponde con la asignación de recursos humanos al tema, es de esperar que con el tiempo dichas asignaciones aumenten.

En que temas se concentra la inversión en Seguridad Informática?

Proteger los datos críticos de la organización	Proteger la propiedad intelectual	Proteger el almac. de datos de clientes	Concientización/ formación del usuario final	Comercio/ negocios electrónicos	Protección de la red	Proteger los datos críticos de la organización
Proteger los datos críticos de la organización	Proteger la propiedad intelectual	12.9%	9.7%	3.2%	12.9%	12.9%
	(en blanco)	12.9%	16.1%	9.7%	41.9%	45.2%
Total Proteger los datos críticos de la organización		25.8%	25.8%	12.9%	54.8%	58%
(en blanco)	Proteger la propiedad intelectual	6.5%			12.9%	
	(en blanco)					
Total (en blanco)		6.5%			12.9%	
Total general		32.3%	25.8%	12.9%	67.7%	58%

Comentarios Generales:

La mayoría de los esfuerzos económicos se centran en proteger los elementos de conectividad de las redes, particularmente en la zona perimetral de las redes y componentes, así como la protección de los datos de los clientes.
En la mayor parte de las organizaciones nacionales no es relevante proteger la propiedad intelectual, probablemente por la escasa producción de investigación a nivel empresarial en nuestro país.
Se destaca también el presupuesto asignado a aumentar la concientización del usuario final dentro de las organizaciones.

Presupuesto previsto para Seguridad Informática:

¿Cuál fue el presupuesto de seguridad informática durante el 2008: gastos, hardware, software, asesorías y sueldos? (elija una, valores en dólares americanos)	Total
En Blanco	16.2%
Entre USD$110.001 y USD$130.000	3.2%
Entre USD$50.001 y USD$70.000	12.9%
Entre USD$70.001 y USD$90.000	6.5%
Más de USD$130.000	16.1%
Menos de USD$50.000	45.2%
Total general	100%

¿Cuál es la proyección del presupuesto total previsto para seguridad informática durante el 2009: gastos, hardware, software, asesorías y sueldos?	Total
En Blanco	16.2%
Entre USD$110.001 y USD$130.000	3.2%
Entre USD$50.001 y USD$70.000	12.9%
Entre USD$90.001 y USD$110.000	3.2%
Más de USD$130.000	16.1%
Menos de USD$50.000	48.4%
Total general	100%

Comentarios generales:

Es preocupante notar que entre "la no existencia de presupuesto" y "menos de U$S 50.000 dólares" se encuentran el 61% de las empresas nacionales.
Esta situación asociada al hecho de que se han consultado referentes de empresas medianas a grandes (representan aproximadamente un 70% de la muestra) de nuestro país, mostraría que si bien se reconoce la importancia de la seguridad para el correcto desempeño de la empresa, todavía no existe el nivel de compromiso en la dirección para afrontar el problema con esfuerzos sostenidos en el tiempo.
Las nuevas legislaciones nacionales en este tema, posiblemente generen las tensiones necesarias en los directorios para que la presente realidad cambie en el futuro, hacia estadios de mayor compromiso.
Lamentablemente en la proyección de 2009, los actores predicen un comportamiento similar al año anterior lo que no estaría cambiando la tendencia.

Nivel de concientización:

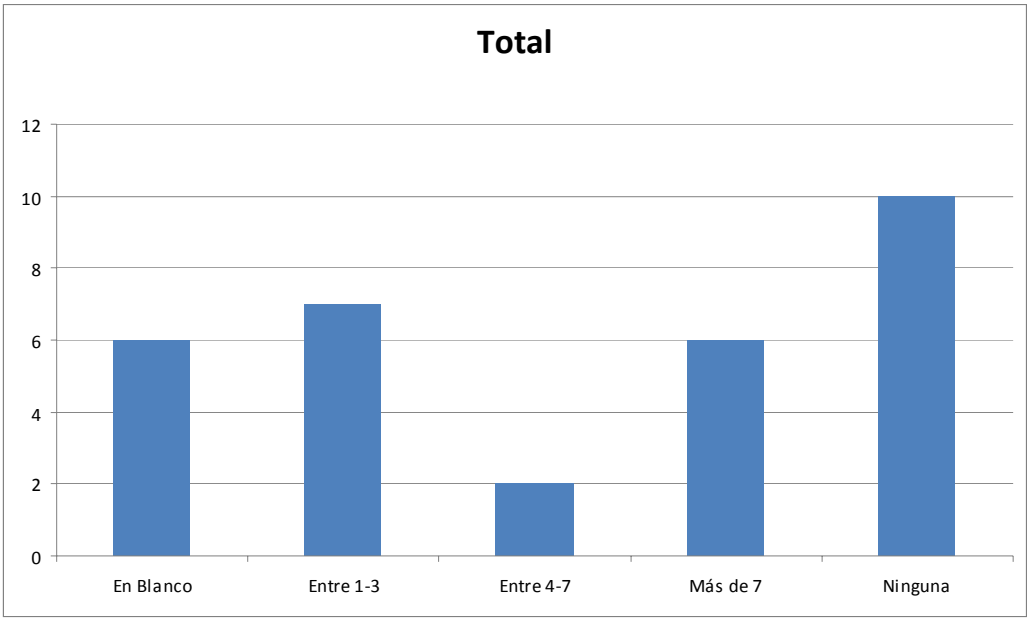
En general, ¿qué tan consciente es su compañía de la seguridad informática (buenas prácticas de seguridad, comunicaciones, redes y seguridad en internet)?	Total
Algunas personas son conscientes	58.1%
En Blanco	19.4%
Muy conscientes	12.9%
Nadie es consciente	6.5%
No sabe	3.2%
Total general	100%

En su organización (todo el personal), ¿se reconoce la información como un activo más a proteger?	Total
En Blanco	16.1%
No	9.7%
Si	32.2%
sólo algunas personas	41.9%
Total general	100%

Comentarios generales:
El nivel de concientización de la importancia de los activos de información ha mejorado sustancialmente en los últimos tiempos en nuestro país, sin embargo no existe la misma difusión de las consecuencias del manejo displicente de las conectividades y conductas de los usuarios en los sistemas y su conectividad a Internet.

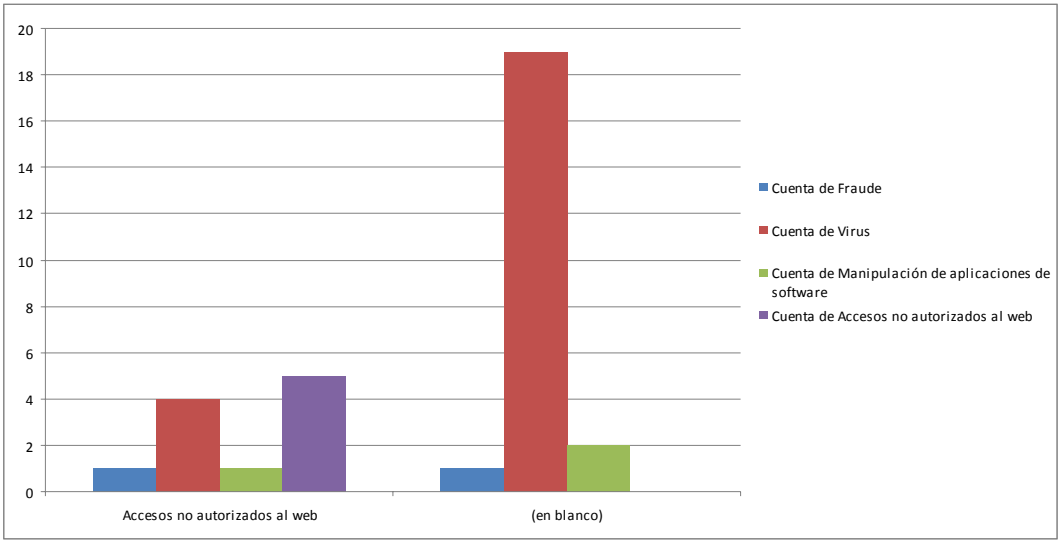
Fallas de Seguridad

¿Cuantas intrusiones o incidentes de seguridad identificó en promedio durante el año anterior?	Total
En Blanco	20.6%
Entre 1-3	22.6%
Entre 4-7	6.5%
Más de 7	19.4%
Ninguna	32.3%
Total general	100%



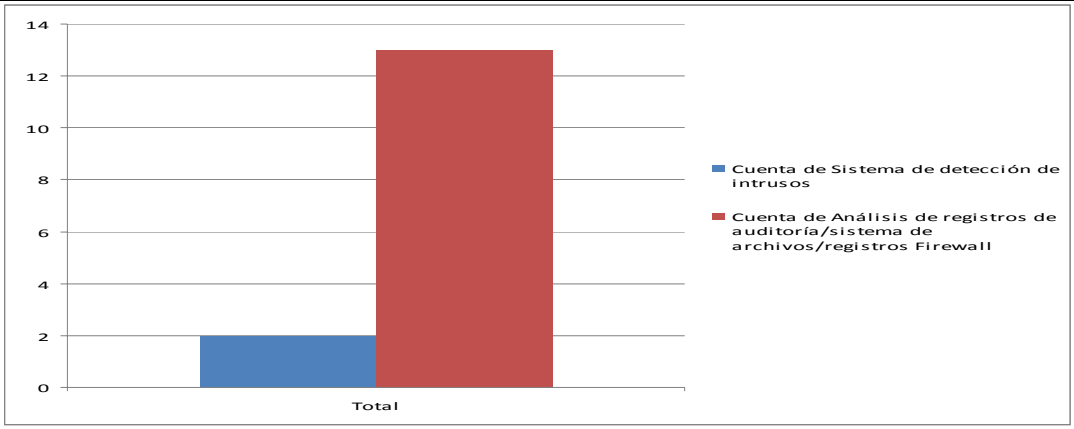
Tipos de incidente

Accesos no autorizados al web	Fraude	Virus	Manipulación de aplicaciones de software	Accesos no autorizados al web
Accesos no autorizados al web	3.2%	12.9%	3.2%	16.1%
(en blanco)	3.2%	61.3%	6.5%	
Total general	6.5%	74.2%	9.7%	16.1%

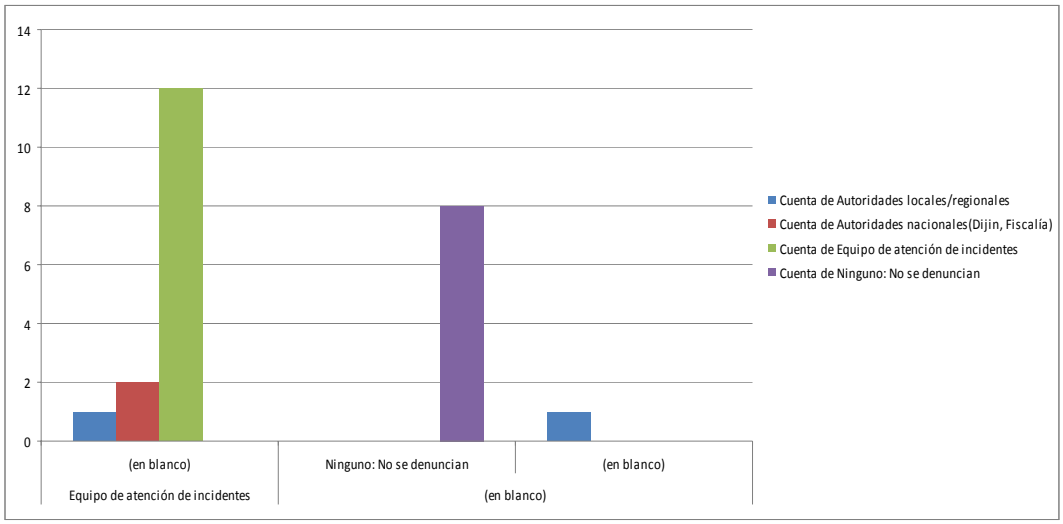


Tipo de detección

	Sistema de detección de intrusos	Análisis de registros de auditoría/sistema de archivos/registros Firewall
Total	6.5%	41.9%



Equipo de atención de incidentes	No se denuncian	Autoridades locales/regionales	Autoridades nacionales	Equipo de atención de incidentes	No se denuncian
Equipo de atención de incidentes	(en blanco)	3.2%	6.5%	38.7%	
Total Equipo de atención de incidentes		3.2%	6.5%	38.7%	
(en blanco)	Ninguno: No se denuncian				25.8%
	(en blanco)	3.2%			
Total (en blanco)		3.2%			25.8%
Total general		6.5%	6.5%	38.7%	25.8%

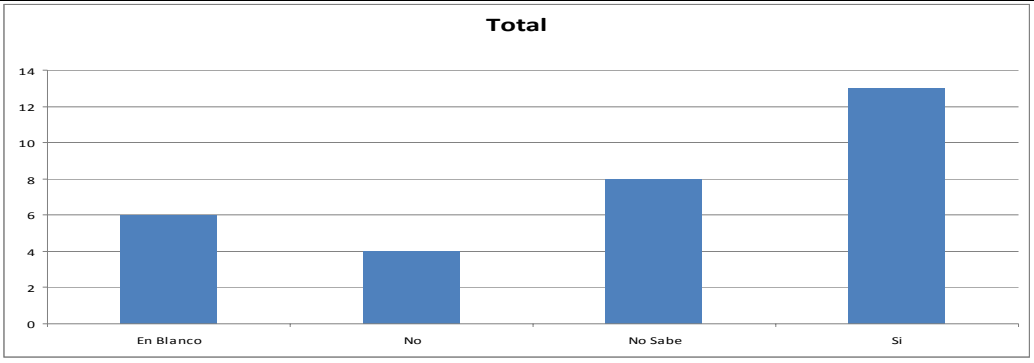


Comentarios generales:

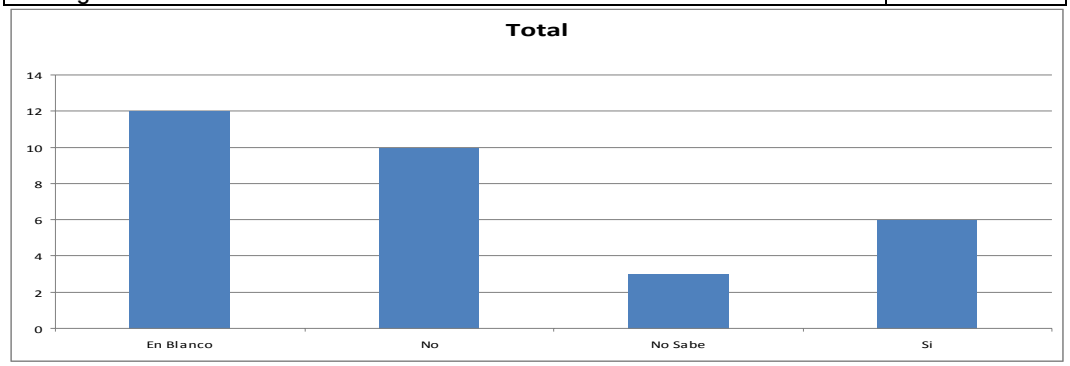
Como se puede observar, la atención a la gestión de incidentes aparece en algunas organizaciones y su existencia provoca una mayor capacidad de la organización de detectar los ataques y actuar en consecuencia.
De todas formas el “no se denuncian” tiene un alto valor 26% que consigna la falta de desarrollo de los equipos de seguridad de alguna de las organizaciones estudiadas, este es un dato preocupante.
Los equipos de IDS y firewalls han sido elementos de la infraestructura que han aportado la información necesaria para detectar las intrusiones o intentos de intrusiones.

Existencia de procesos de manejo de evidencia digital

¿Su organización es consciente de que existe evidencia digital que debe ser identificada, asegurada y analizada, como parte del proceso de atención de incidentes de seguridad informática?	Total
En Blanco	19.4%
No	12.9%
No Sabe	25.8%
Si	41.9%
Total general	100%



Si respondió afirmativamente a la pregunta 20, ¿la organización cuenta con un procedimiento aprobado y verificado para la administración de la evidencia digital?	Total
En Blanco	38.7%
No	32.3%
No Sabe	9.7%
Si	19.4%
Total general	100%

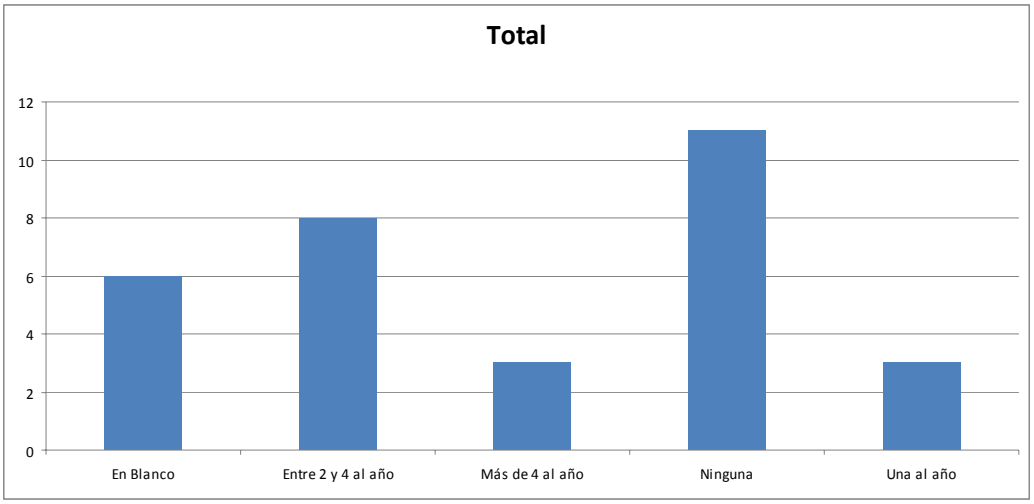


Comentarios Generales

Como se desprende de lo mostrado arriba menos del 20% tiene documentados procesos de recolección de evidencia digital. En nuestro país la legislación sobre este tema es muy vaga y la actuación de los jueces ha sido errática y poco exigente.
Esta situación genera el bajo nivel de desarrollo en las organizaciones nacionales.

Procedimientos de Seguridad

Durante el año anterior ¿cuántas pruebas de seguridad realizó su organización para valorar el estado de seguridad informática? (elija una)	Total
En Blanco	19.4%
Entre 2 y 4 al año	25.8%
Más de 4 al año	9.7%
Ninguna	35.5%
Una al año	9.7%
Total general	100%

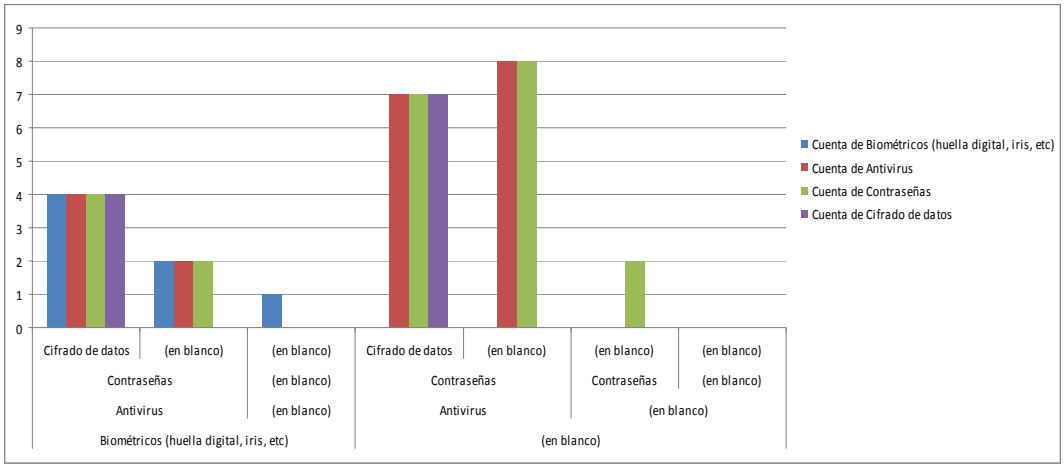


Comentarios generales

El 64% de las empresas han estado realizando pruebas de seguridad de sus plataformas al menos una vez al año, sin embargo sólo el 36% han realizado más de una prueba, evidenciando una actividad sostenida de seguridad.

Mecanismos de seguridad

Biométricos (huella digital, iris, etc)	Antivirus	Contraseñas	Cifrado de datos	Biométricos (huella digital, iris, etc)	Antivirus	Contraseñas	Cifrado de datos
Biométricos (huella digital, iris, etc)	Antivirus	Contraseñas	Cifrado de datos	12.9%	12.9%	12.9%	12.9%
			(en blanco)	6.5%	6.5%	6.5%	
		Total Contraseñas		19.4%	19.4%	19.4%	12.9%
	Total Antivirus			19.4%	19.4%	19.4%	12.9%
	(en blanco)	(en blanco)	(en blanco)	3.2%			
		Total (en blanco)		3.2%			
	Total (en blanco)			3.2%			
Total Biométricos (huella digital, iris, etc)				22.6%	19.4%	19.4%	12.9%
(en blanco)	Antivirus	Contraseñas	Cifrado de datos		22.6%	22.6%	22.6%
			(en blanco)		25.8%	25.8%	
		Total Contraseñas			48.4%	48.4%	22.6%
	Total Antivirus				48.4%	48.4%	22.6%
	(en blanco)	Contraseñas	(en blanco)			6.5%	
		Total Contraseñas				6.5%	
		(en blanco)	(en blanco)				
		Total (en blanco)					
	Total (en blanco)					6.5%	
Total (en blanco)					48.4%	54.8%	22.6%
Total general				22.6%	67.8%	74.2%	35.5%

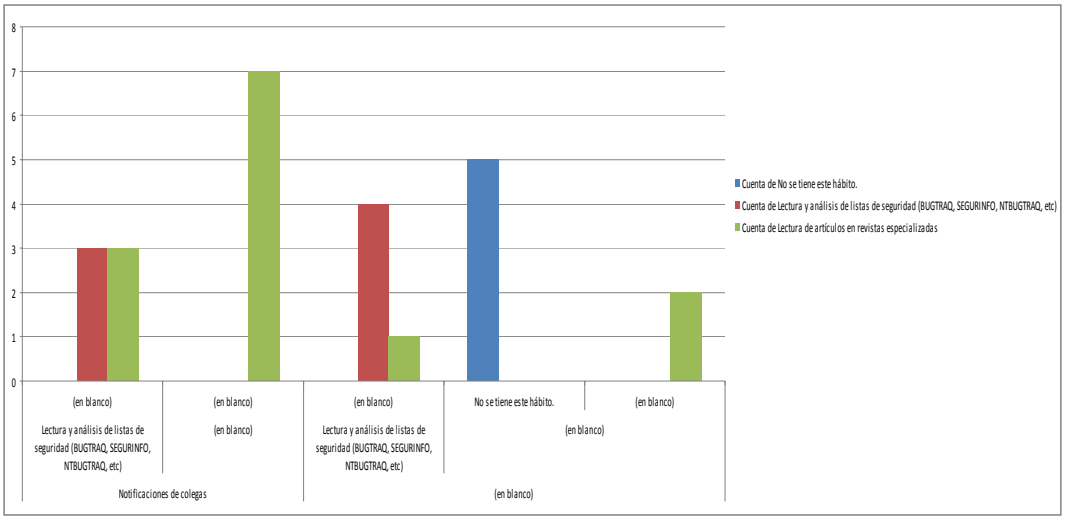


Conclusiones:

Las respuestas nos muestran que las contraseñas, antivirus y dispositivos biométricos son los más utilizados a la hora de resolver problemas de seguridad y control de accesos. Dichas tendencias son semejantes a las presentadas en 2007 por CSI/FBI Computer Crime and Security, en el cual se presentan como las tecnologías más usadas: los antivirus, firewalls, VPN y antispyware. Existe un importante interés en el cifrado de datos y las herramientas asociadas.

¿Cómo se entera de las fallas de seguridad?

Notificaciones de colegas	Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc)	No se tiene este hábito.	No se tiene este hábito.	Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc)	Lectura de artículos en revistas especializadas
Notificaciones de colegas	Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc)	(en blanco)		9.7%	9.7%
	Total Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc)			9.7%	9.7%
	(en blanco)	(en blanco)			22.6%
	Total (en blanco)				22.6%
Total Notificaciones de colegas				9.7%	32.3%
(en blanco)	Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc)	(en blanco)		12.9%	3.2%
	Total Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc)			12.9%	3.2%
	(en blanco)	No se tiene este hábito. (en blanco)	16.1%		6.5%
	Total (en blanco)		16.1%		6.5%
Total (en blanco)			16.1%	12.9%	9.7%
Total general			16.1%	22.6%	41.9%

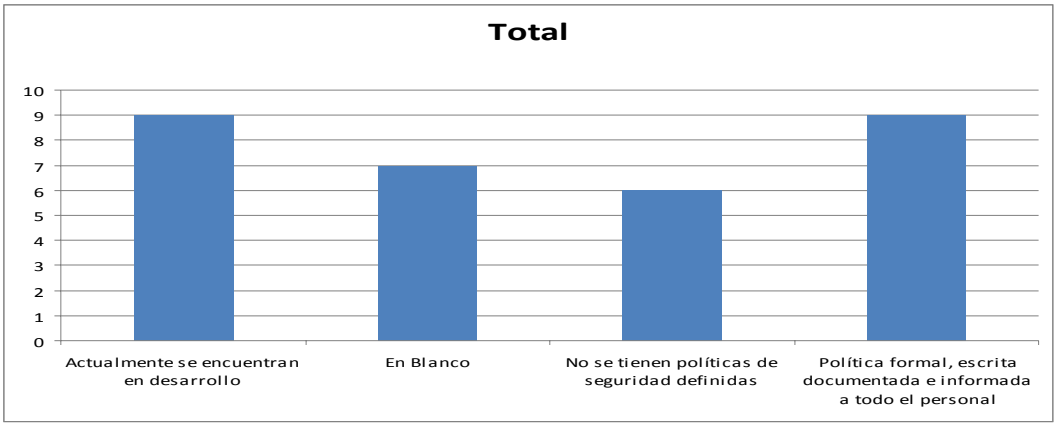


Comentarios generales:

La lectura y participación en listas especializadas en seguridad informática son las fuentes de información mas frecuentes para notificarse sobre fallas de seguridad, luego sigue la lectura en revistas especializadas.
Se visualiza la aparición de un tiempo en las agendas para el estudio permanente de la dinámica de seguridad, así como para mejorar la comprensión y revisión de las fallas de seguridad y su impacto en la organización.

Políticas de Seguridad

¿Qué describe mejor la política de seguridad de su organización? (elija una)	Total
Actualmente se encuentran en desarrollo	29%
En Blanco	22.6%
No se tienen políticas de seguridad definidas	19.4%
Política formal, escrita documentada e informada a todo el personal	29%
Total general	100%



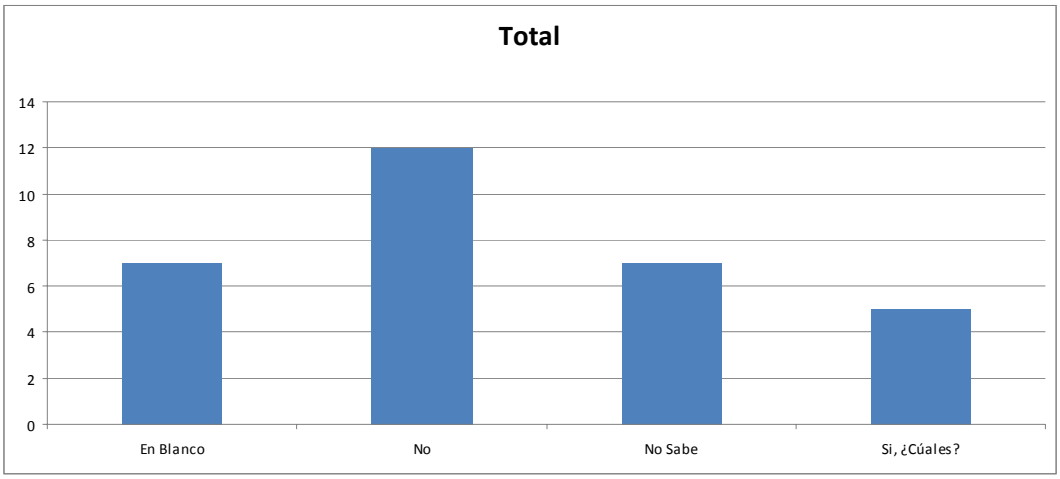
Comentarios generales:

El 71% de las empresas en Uruguay no cuentan con políticas de seguridad definidas formalmente o se encuentran en desarrollo. Es necesario promover entonces estas

actividades dado que la seguridad de la información por reacción es mucho más costosa, tanto en recursos como en riesgos de afectación de imagen o pérdidas directas. La existencia de un Sistema de Gestión de Seguridad de la Información articulado con las necesidades de negocio genera mucho más valor y permite asimilar mejor las fallas de seguridad que se presenten.

Escalamiento de incidentes, puntos de contacto

¿Actualmente su organización posee contactos o relaciones con autoridades nacionales e internacionales para colaborar y recibir asistencia en casos de persecuciones de intrusos?	Total
En Blanco	22.6%
No	38.7%
No Sabe	22.6%
Si, ¿Cúales?	16.1%
Total general	100%

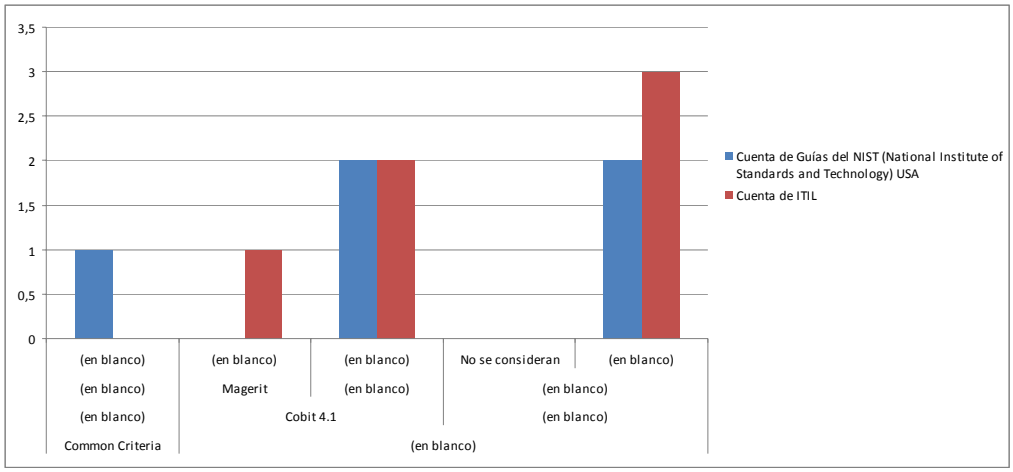


Conclusiones:

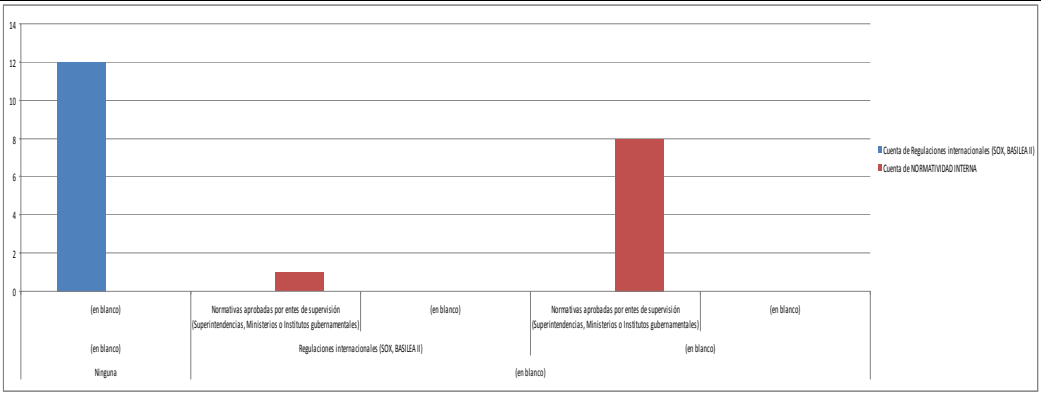
El 84% de los encuestados no tiene identificado ningún punto de contacto para escalar un incidente informático, esto es debido a que en el momento de realizarse la encuesta aún no estaba operativo el CERT.uy de reciente creación. El mismo es el punto de contacto del Estado Uruguayo. Adicionalmente para grandes entidades privadas, en el 2006 se ha creado el CSIRT de ANTEL, de la telefónica estatal de Uruguay.
Estos puntos aún no han sido reconocidos, pero es de esperar que con el transcurso del tiempo y las acciones que tienen para emprender en su desarrollo estas organizaciones de respuesta a incidentes, lograrán aumentar la difusión y relevancia entre los actores de TI a nivel nacional.

Estándares y buenas prácticas en Seguridad Informática y Regulaciones en Seguridad de la Información

Common Criteria	Cobit 4.1	Magerit	No se consideran	Cuenta de Guías del NIST (National Institute of Standards and Technology) USA	Cuenta de ITIL
Common Criteria	(en blanco)	(en blanco)	(en blanco)	3.2%	
		Total (en blanco)		3.2%	
	Total (en blanco)			3.2%	
Total Common Criteria				3.2%	
(en blanco)	Cobit 4.1	Magerit	(en blanco)		3.2%
		Total Magerit			3.2%
		(en blanco)	(en blanco)	6.5%	6.5%
		Total (en blanco)		6.5%	6.5%
	Total Cobit 4.1			6.5%	9.7%
	(en blanco)	(en blanco)	No se consideran		
			(en blanco)	6.5%	9.7%
		Total (en blanco)		6.5%	9.7%
	Total (en blanco)			6.5%	9.7%
Total (en blanco)				12.9%	19.4%
Total general				16.1%	19.4%



Regulaciones internacionales (SOX, BASILEA II)	Normativas aprobadas por entes de supervisión (Superintendencias, Ministerios o Institutos gubernamentales)	NORMATIVIDAD INTERNA	Cuenta de Regulaciones internacionales (SOX, BASILEA II)	Cuenta de NORMATIVIDAD INTERNA
Ninguna	(en blanco)	(en blanco)	38.7%	
	Total (en blanco)		38.7%	
Total Ninguna			38.7%	
(en blanco)	Regulaciones internacionales (SOX, BASILEA II)	Normativas aprobadas por entes de supervisión (Superintendencias, Ministerios o Institutos gubernamentales)		3.2%
	Total Regulaciones internacionales (SOX, BASILEA II)			3.2%
	(en blanco)	Normativas aprobadas por entes de supervisión (Superintendencias, Ministerios o Institutos gubernamentales)		25.8%
	Total (en blanco)			25.8%
Total (en blanco)				29%
Total general			38.7%	29%

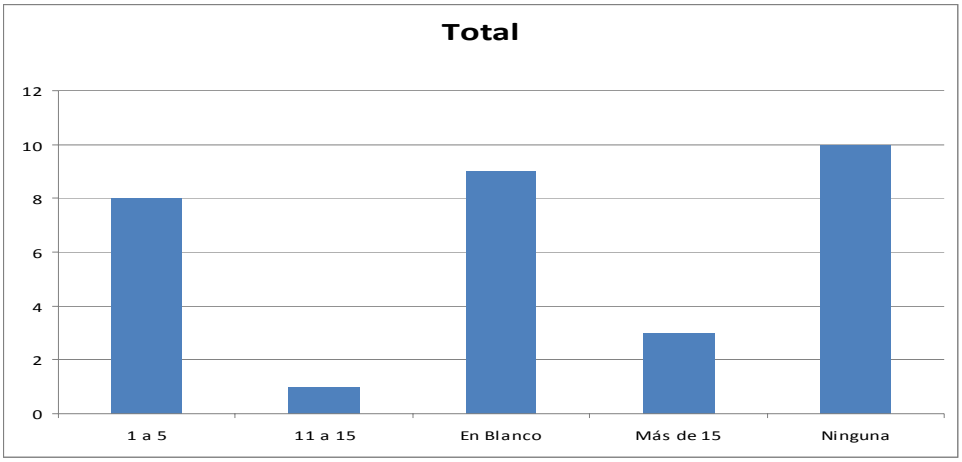


Conclusiones generales:

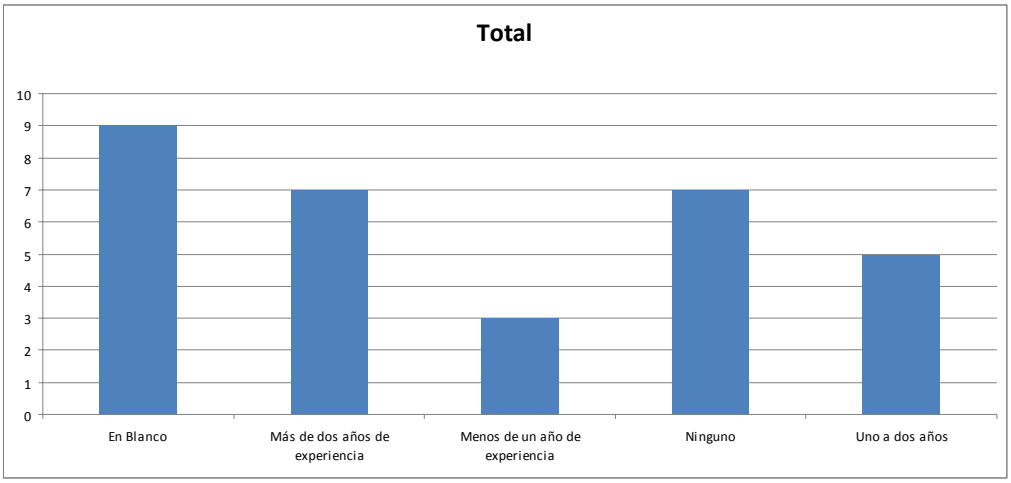
En Uruguay, se ha exigido por normativa del Banco Central evaluar el cumplimiento de seguridad en TI a través de COBIT. Por lo que se puede ver en las respuestas salvo SOX no está establecido aún ningún estándar con predominancia.

Acerca de las personas dedicadas a seguridad informática

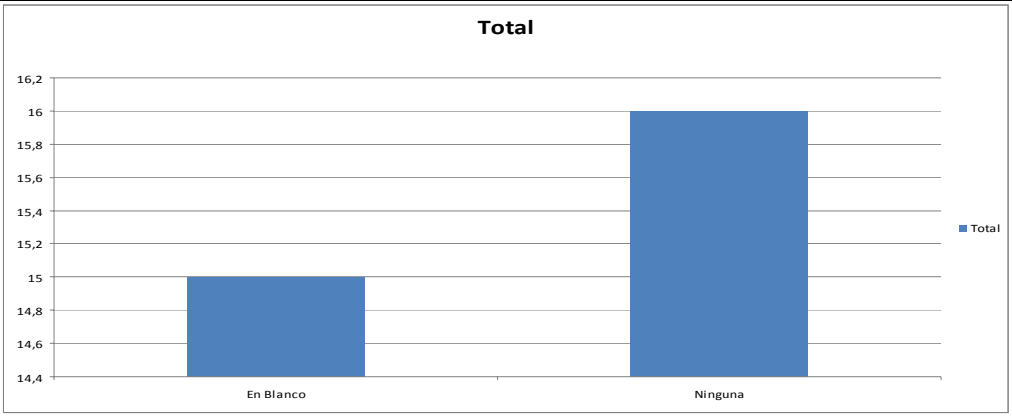
¿Cuántas personas de tiempo completo o equivalente se dedican a la seguridad informática?	Total
1 a 5	25.8%
11 a 15	3.2%
En Blanco	29%
Más de 15	9.7%
Ninguna	32.3%
Total general	100%



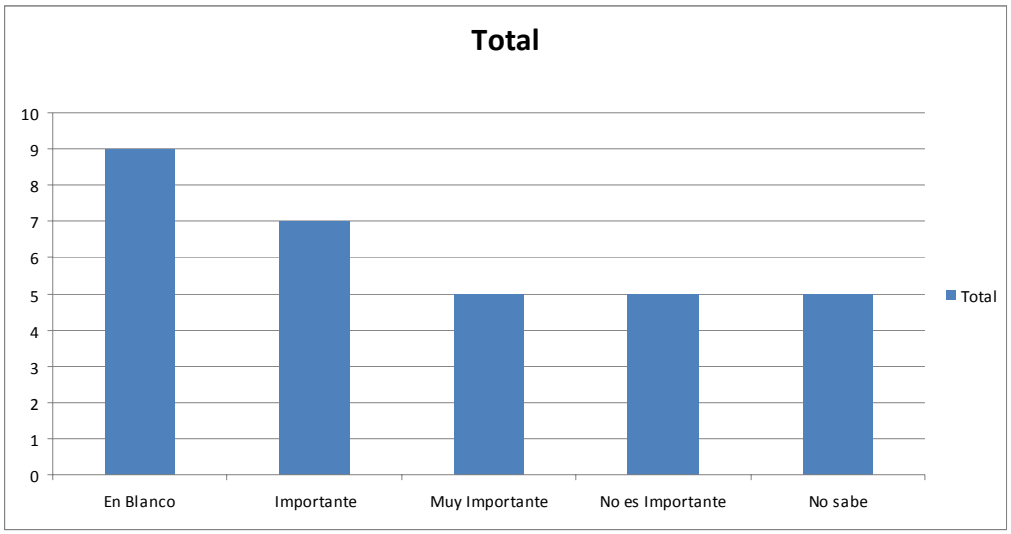
¿cuántos años de experiencia mínima requiere una persona para obtener un cargo en el área de seguridad informática?	Total
En Blanco	29%
Más de dos años de experiencia	22.6%
Menos de un año de experiencia	9.6%
Ninguno	22.6%
Uno a dos años	16.1%
Total general	100%



Basado en las 2 respuestas anteriores, marque las certificaciones relacionadas con seguridad de la información que poseen los profesionales dedicados a estos temas, en su organización.	Total
En Blanco	48.4%
Ninguna	51.6%
Total general	100%



¿Qué tan importante es para usted que el personal dedicado a la seguridad informática de su compañia tenga alguna de las siguientes certificaciones?	Total
En Blanco	29%
Importante	22.6%
Muy Importante	16.1%
No es Importante	16.1%
No sabe	16.1%
Total general	100%



Comentarios:

Existe en el mercado falta de personas calificadas, debido a la falta de experiencia en el tema, así como la total ausencia de programas académicos de seguridad en las formaciones de grado. Recientemente (hace menos de dos años) se han formado algunas propuestas de postgrado en la Universidad de la República.

Conclusiones generales:

Los resultados sugieren las siguientes reflexiones:

- Las regulaciones nacionales e internacionales llevarán a las organizaciones a fortalecer y en algunos casos establecer los sistemas de seguridad de la información.
- La falta de ofertas de programas académicos formales en nuestro país limita seriamente el desarrollo de un mercado de especialistas en el sector. Esto provoca la aceptación por parte de las empresas de la inclusión de personas sin experiencia en el desarrollo de las tareas.
- Las certificaciones CISSP, CISA y CISM son las mas valoradas por el mercado.
- La inversión en seguridad de la información se encuentra concentrada en las redes y sus componentes, luego en la protección de los datos de sus clientes.
- Las cifras muestran a las contraseñas, antivirus y firewalls como los mecanismos de seguridad mas utilizados. Existe un importante interes por el cifrado de datos.

1.