- Capital
- Competidores
- Capacitados
- Política

La confidencialidad es uno de los pilares más importantes de la Seguridad Informática. Tiene que ver con el aseguramiento de que la información sólo sea accedida, revisada, consultada, por usuarios con la debida autorización. Es decir, que se mantenga bajo un manto de protección que sólo sea descubierto por quienes deben hacer un uso responsable y auténtico de dicho recurso. Las Empresas manejan gran cantidad de información propia de su negocio, y que sea propia hace que la confidencialidad sea un factor clave a la hora de protegerla.
El concepto íntegro tiene que ver con los sistemas que las Empresas utilizan procurando que los mismos se mantengan en estado correcto, con la información en su estado original, asegurando que la misma no sufra alteraciones y esté disponible cuando se la necesite y por las personas con permisos para eso. Aquí aparece el término disponibilidad, constituyendo otro de los pilares fundamentales para tener información segura.
Para poder implementar un plan de seguridad de la información es necesario contar con un conjunto de normas y procedimientos que se sigan y cumplan en todos los niveles de la organización. Tiene que ver con contar con una línea de trabajo que incorpore en cada una de las acciones el valor por la información.
Más allá del concepto de pérdida económica presente en todo negocio de una empresa, surge la problemática de la pérdida de información. Las Empresas están considerando a la información como un activo esencial para su desarrollo siendo fundamental a la hora de lograr ventajas competitivas. Por eso es lógico que las pérdidas ya no sólo se evalúen a nivel económico sino a nivel información. Podemos decir que ésta forma parte del capital de toda empresa y cuanto mayor y de mejor calidad sea, marcará una diferencia con los demás competidores. Contar con análisis de mercados, comportamientos de los clientes, resultados de simulaciones, datos históricos, hacen que una Empresa tenga un capital en información importante que la lleve a mejorar su productividad y su influencia en el mercado.
Debemos destacar que los empleados tienen la posibilidad de estar más capacitados en el uso de las nuevas tecnologías y principalmente por la incidencia que esta tiene en la vida cotidiana. Internet es una fuente infinita de recursos informativos de todo tipo por lo que hace que toda persona pueda investigar y conocer muchos temas. Esto logra que los usuarios se hagan más conscientes sobre el valor de la información que manejan y a su vez se dan cuenta de la facilidad de acceso a todos esos recursos. Por eso una buena política de capacitaciones para los empleados en el correcto uso y administración de la información, resulta ser de suma importancia para toda Empresa.
Un aspecto muy importante para destacar es que el **90%** de las Empresas encuestadas le asigna un valor importante a la Información Digital que genera. El **10%** restante le brinda un valor moderado. Lo interesante es que ninguna de ellas indica un valor mínimo lo que pone de manifiesto que la Información es un activo considerado en todas las organizaciones y que está bajo continuo seguimiento por parte de las mismas.
Hoy en día es prácticamente improbable que una empresa desconozca el concepto de seguridad informática. De alguna u otra manera, la idea de proteger sus datos está presente. Después lo que varía es si realmente aplica un plan concreto de seguridad.

¿Su empresa tiene un plan de Seguridad de la Información Digital implementado?
En este sentido destacamos que el **74%** de las Empresas tiene un plan de Seguridad de la Información Digital implementado. Los motivos principales que argumentan esta decisión son:

- Importancia para el desarrollo.
- Para lograr que el sistema cumpla con los requisitos enumerados en el ítem 2
- Porque generaría un caos perderla y sería muy difícil (prácticamente imposible) recuperarla
- Por privacidad y protección
- Por la importancia y valor de la información.
- Por los riesgos de filtración y fraude.
- Para no generar pérdidas de la misma en desarrollos
- Para asegurar su disponibilidad en todo momento.
- Todo lo que se genera es digital y es el corazón de la empresa.
- La información es el principal activo.

Debemos comentar que el resto de las empresas, si bien no tienen definido un plan global de seguridad informática, cuentan con medidas básicas para proteger este recurso. Esto es importante, porque más allá de que sea básico, habla de un interés por el recurso información y quizás sea la antesala para un plan integral de seguridad.

¿Su Empresa se interesa en participar de Charlas / Cursos / Seminarios sobre Seguridad de la Información Digital?

Analizando este punto de las encuestas notamos que aproximadamente el **50%** de las Empresas tienen interés en participar de capacitaciones relacionadas a la Seguridad de la Información. Es un aspecto a tener en cuenta porque consideramos que la primera instancia para reconocer la importancia de la seguridad en los activos de la información se obtiene cuando se recibe información proveniente de cursos, charlas, campañas de concientización y todo lo que provenga de especialistas del tema. A partir de las mismas, la Empresa puede empezar a diagramar su plan de seguridad, contemplando todos los aspectos fundamentales. Quizás lo más importante sea que la Empresa pueda conocer su estado, es decir, su radiografía que muestre la situación frente a la protección de la información.

De 1 a 5 en orden creciente de importancia, ¿Cómo califica el uso del Correo Electrónico en su empresa?

El **74%** de las Empresas le dan el máximo nivel de importancia al uso del correo electrónico. Considerando una escala de 1 a 5, la mayoría de las organizaciones le pone un valor de 5 al uso de esta herramienta de comunicación. La información es el principal recurso que fluye por medio del correo, y no sólo estamos hablando de datos propios del negocio de le empresa, sino de cuestiones personales de cada uno de los usuarios. Con esta proporción de respuestas, evidenciamos por donde se canaliza el mayor volumen de datos en la empresa y hacia donde se debería orientar un plan de seguridad de la información.

¿Poseen normas reglamentarias sobre el uso de Correo Electrónico?

Aproximadamente el **50%** de las empresas posee un desarrollo de normas reglamentarias sobre el uso del Correo Electrónico. En un punto anterior se ponía de manifiesto que para la mayoría de ellas el correo tiene una importancia considerable en el desarrollo de su trabajo. Con esta respuesta, vemos que sin embargo, eso no significa que concretamente la empresa esté administrando el correcto uso de este recurso. Entendemos que el correo es un factor clave de comunicación de información en toda organización de tipo empresaria, no sólo de datos propios del negocio sino también de cuestiones personales de cada uno de los usuarios. Por eso los datos que se manejan pueden exceder los dominios de la empresa. Contar con una reglamentación en el uso de este servicio, permite que la empresa pueda especificarle al usuario, qué usos son los correctos para el correo definiendo los límites necesarios y los

controles que se podrían aplicar en el caso que sea requerido. Así mismo, por medio de una reglamentación que el usuario conozca y apruebe de antemano, la empresa tendrá una protección legal frente a cuestiones que se deriven de situaciones de control y auditoría sobre correos que puedan pertenecer a sus empleados y que requieran ser analizados debido a una situación que infrinja la seguridad de la información.

¿Su empresa realiza controles sobre todas las cuentas de correo electrónico?

Las respuestas a esta pregunta indican que el **70%** de las empresas no realizan controles sobre las cuentas de correo electrónico.

Pueden plantearse varios puntos de vista en relación a este resultado pero principalmente nos orientamos a qué llevar a cabo un control de los correos, implica acceder a contenido de información propia de cada miembro de la empresa y eso no es un tema menor. Generalmente las empresas se basan en las normas que definieron sobre el uso del correo y la aceptación de las mismas por parte de su personal. Eso de alguna manera genera cierta confianza sobre el uso de esta herramienta de comunicación. Así mismo, se debe considerar que controlar una determinada cuenta de correo significa romper la privacidad que el propietario tiene sobre la misma. Por eso es muy frágil el límite entre controlar las cuentas de correo y dejar sin efecto la confidencialidad de los mensajes de correo. Tiene que existir una justificación apropiada para llevar adelante un control de los correos para no incurrir en la violación de otras propiedades de la información personal.

En caso de que la pregunta anterior haya sido afirmativa: ¿Su empresa informa que ejercerá estos controles?

En este caso, la totalidad de las empresas indican que informan a su personal que realizarán controles sobre las cuentas de correo. Es un factor muy importante porque se trata de analizar correos que son propios de cada integrante de la organización y por eso se tiene el derecho de conocer cuando se accederá a esos recursos. Así mismo permite que se puedan plantear objeciones a la medida con la realización de una correcta justificación al respecto.

¿Se permite su empresa el uso de dispositivos de almacenamiento portátil como pendrives, discos externos, etc.?

El **70%** de las empresas indican que permiten el uso de dispositivos portátiles de almacenamiento. El desarrollo de la tecnología permite la existencia de un sin número de mecanismos para compartir información de manera electrónica. Directamente con cualquier celular se puede desarrollar una red de comunicación para manejar información. Existen mecanismos para bloquear el acceso a los puertos USB de las computadoras, pero no son controles con tengan una eficacia absoluta. Existen técnicas para romper con esa restricción.

De todos modos debemos destacar que se debe trabajar sobre la conciencia en el uso de la información de la empresa. Hasta tanto no se logre transmitir del valor que tiene la información que se maneja en una organización siempre existirán mecanismos para poder compartir dicho recurso por fuera de los ámbitos del negocio.

¿Tuvieron situaciones en las cuáles se puso en riesgo la Seguridad de la Información digital?

Esta pregunta la consideramos importante a la hora de evaluar la situación de una empresa frente a la seguridad de la información. Aproximadamente el **25%** de la organizaciones encuestadas tuvieron una situación donde la información fue víctima de violaciones en su seguridad.

Entre las situaciones indicadas se pueden mencionar:

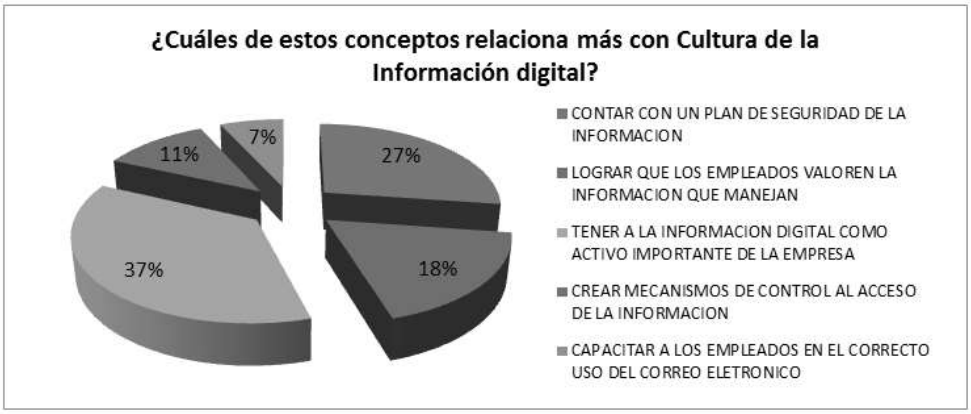
- Virus en pendrive.
- Empleados deshonestos.

- Infección por Troyanos en dispositivos de almacenamiento portátil.
- Acceso de empleados a computadoras sin la debida autorización.
- Pérdida de correos electrónicos de una casilla central.
- Problemas con el disco de almacenamiento de los Backups centrales.

El uso de los dispositivos portátiles es corriente y es el motivo principal para el ingreso de Virus o Troyanos. Debemos aclarar el significado de este tipo de aplicaciones dañinas llamadas Troyanos. Para ello tomamos la definición de Panda Security, un reconocido desarrollador de programas antivirus:
"Los Troyanos son programas que se ejecutan en una determinada computadora con el objetivo de introducir e instalar otras aplicaciones en ese equipo infectado, para permitir su control remoto desde otros equipos. Llegan al equipo del usuario como un programa aparentemente inofensivo."
Otro concepto para destacar es el del "empleado deshonesto". Está comprobado que las principales amenazas en seguridad de la información en una empresas están dentro de ellas. La justificación es clara: el personal de la organización tiene acceso a la información del negocio y su situación de empleada brinda un marco de confianza sobre el uso de este recurso orientando las amenazas para fuera de los límites de la empresa. Por eso, no es para asustarse que sea desde dentro de la empresa donde se gesten las situaciones que alteren la seguridad de la información.
Si bien el porcentaje de empresas que tuvieron este tipo de situaciones es bajo, resulta suficiente para dejar vulnerable a la información. Las empresas que indicaron que no tuvieron estos acontecimientos pueden ser víctimas en un futuro o tal vez todavía no se han dado cuenta de la ocurrencia de las mismas.

¿Cuáles de estos conceptos relaciona más con Cultura de la Información digital?

- Contar con un plan de seguridad de la información
- Lograr que los empleados valoren la información que manejan
- Tener a la información digital como activo importante de la empresa
- Crear mecanismos de control al acceso de la información
- Capacitar a los empleados en el correcto uso del correo electrónico



Los tres conceptos que las empresas consideran más relacionados con la Cultura de la Información Digital son:

- Contar con un plan de seguridad de la información
- Tener a la información digital como activo importante de la empresa
- Lograr que los empleados valoren la información que manejan

De estos tres, las empresas indicaron que "tener a la información digital como activo importante de la empresa" constituye el factor más relacionado con contar con una Cultura de

la Información Digital. Es importante la elección de este concepto ya que demuestra que las empresas consideran a la información como un activo importante en la empresa. Ya es importante que se catalogue a la información como un activo. Con esa base, considerándola como un bien, se puede abordar una política sobre seguridad de la información integral.
Contar con un plan de seguridad de la información también es importante y por eso fue el segundo en ser seleccionado. De todos modos tenemos que considerar que la cultura de la información digital no se consigue solamente con un plan de seguridad implementado sino que va más allá, involucrando a todos los actores que forman parte de la organización y logrando que cada empleado entienda la importancia de hacer un uso adecuado de la información. Esto habla del tercer concepto elegido en importancia por todas las empresas en esta pregunta de la encuesta. Consideramos que lograr que los integrantes de las organizaciones valoren a la información forma los cimientos fundamentales para construir una cultura sobre la información digital.

¿Puede nombrar y/o ejemplificar los delitos informáticos que conozca?
Las empresas indicaron los siguientes ejemplos de delitos informáticos que conocen:

- Hackeo de sitios con robo de información.
- Ataques externos o internos a los sistemas de información
- Robo de identidad de usuarios
- Spam, Spywares y Pishing
- Publicación de información de personas
- Borrado de información
- Fraude
- Contenidos obscenos u ofensivos
- Violación de derechos de autor
- Ingreso ilegal a sistemas
- Interferencias de redes
- Suplantación de identidad
- Daños a la información
- Venta de base de datos confidenciales
- Hackeo de correos electrónicos
- Virus
- Transferencia de información a la competencia
- Terrorismo virtual
- Piratería
- Chantaje y falsificación
- Acceso a información sin autorización
- Robo de contraseñas

¿Sabe que su empresa dispone de mecanismos legales que la amparen contra delitos informáticos?
En esta pregunta, aproximadamente el 75% de las empresas expresaron que no conocen la existencia de mecanismos legales que las amparen frente a los delitos informáticos. Queda de manifiesto que no se tiene conocimiento de las herramientas legales vigentes en nuestro país en materia de delitos informáticos. Se advierte en este sentido la necesidad de que los Departamentos Legales de las Empresas (para aquellos que lo tengan) se capaciten al respecto. Dicha capacitación debe versar, en la cuestión de fondo, es decir en el contenido de la ley a los fines de detectar acciones que puedan constituir Delitos; como así también en la cuestión de forma, a saber, como proceder ante la sospecha o el acaecimiento de una acción

que pueda configurar un delito. En este sentido cabe señalar: formular la denuncia, como formularla, ante que autoridad, como resguardar las pruebas, etc.-

A la pregunta: **¿Conoce la nueva Ley denominada de Delitos Informáticos sancionada en el año 2008 y que introduce modificaciones a nuestro Código Penal?** El **70 %** de las empresas encuestadas contesto que no. Cabe señalar en este sentido que, dicha ley que data del año 2008, actualiza nuestro Código Penal conforme las nuevas tecnologías, protegiendo de esta manera la infraestructura tecnológica de las empresas. Desde la perspectiva de la técnica legislativa empleada, el legislador ha acudido a la instrumentación de una ley de reforma integral y concordada del Código Penal y no ha recurrido al empleo de una ley complementaria. Como consecuencia de ello, no se crean nuevos tipos penales, sino que se modifican ciertos aspectos de los ya contemplados, cumpliendo así su objetivo de receptar y captar las nuevas tecnologías como medios comisivos para su ejecución. Se habla así de un Modelo Político Criminal Reductor del poder punitivo. Asimismo la ley 26.388, según los doctrinarios, se orienta a un derecho penal de acto, ya que en forma directa se dirige a reglar las conductas o acciones susceptibles de sanción penal, así en ninguno de sus tipos penales ha recurrido al empleo de una biotipología de autores de la criminalidad informática como pueden ser las designaciones de Hacker, Craker, Preaker, Phisher, Sniffer, Virucker, Propagandista Informático, Pirata informático, Ciber-Acosador, etc.-

¿En alguna oportunidad su empresa fue víctima de un delito informático?
El **70%** de las empresas contestó que no, el 4% que sí y el 24 % que no sabía.-
Al respecto manifestamos que de la lectura de Jurisprudencia referida a la comisión de Delitos Informáticos se ha podido inferir que muchos de ellos, luego de ser investigados, resultan atípicos ya que por principio de especialidad no pueden ser subsumidos bajo estos tipos penales. No obstante en el mismo orden de ideas, la Ley 26388 de reforma en materia de criminalidad informática al Código Penal no incorpora ningún tipo omisivo, ni doloso, ni culposo, lo cual debe destacarse en un Estado de Derecho y respetuoso del principio de reserva y de legalidad de los ciudadanos. Como contrapartida los delitos que han llegado a tipificarse y posteriormente han sido pasibles de condena son a título de ejemplo: DELITOS CONTRA LA LIBERTAD - Violación de secretos - Violación de correspondencia y papeles privados. También, la nueva ley sanciona a quien alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daño (daño Informático). En esta figura encuadran los virus informáticos.

¿Su empresa cuenta con una política de privacidad?
El **57%** de las empresas contesto afirmativamente, mientras que el **43 %** lo hizo por la negativa. Cabe destacar aquí que una de las principales incorporaciones de la Ley 26.388 es la equiparación del correo electrónico a la correspondencia epistolar, limitándose de esta manera el acceso al mismo. La ley incluye dentro del concepto amplio de "correspondencia" a las comunicaciones electrónicas solucionando por vía judicial las controversias generadas en la doctrina y la jurisprudencia sobre la posibilidad de asimilar al correo electrónico (e-mail) a la correspondencia tradicional. De esta manera se advierte la imperiosa necesidad, tal como ya afirmáramos, de que las empresas formulen políticas de privacidad (El **57%** de las empresas encuestadas contesto que sí, mientras que el **43%** contesto que no) que de forma clara y definida informe a los empleados cuales son los límites en el uso de las herramientas tecnológicas de la empresa, y cuáles son las consecuencias; el control que realizará sobre el correo electrónico y como lo hará, ya que un acceso indebido a los sistemas informáticos es ahora delito.

¿Su empresa cuenta con un departamento jurídico y/o legal?
El **57 %** de las empresas contesto que no, mientras que el **43 %** lo hizo por la afirmativa.

5. Conclusión

Una de las cuestiones que este proyecto de investigación ha puesto de manifiesto es la necesidad del trabajo interdisciplinario. Los conceptos vinculados a la Seguridad de la Información están en constante vínculo con las Ciencias Jurídicas y de allí la necesidad de un trabajo mancomunado y solidario entre ambas disciplinas. Las empresas encuestadas ponen de manifiesto que la información es un activo importante y que está bajo continuo seguimiento. Es prácticamente improbable que una empresa desconozca el concepto de seguridad de la información. La idea de proteger sus datos está presente, poniendo énfasis en la información que los empleados administran, en cómo la misma es protegida y en los riesgos posibles. Consideramos de vital importancia que las empresas inicien un plan concreto de capacitaciones en cuanto a la administración adecuada de la información, exponiendo a todos sus miembros, los conceptos que permiten hacer a este bien seguro y protegido frente a toda posible amenaza de manera de lograr una cultura de la información digital.

Referencias

ABOSO, GUSTAVO EDUARDO- ZAPATA, MARIA FLORENCIA: “Cibercriminalidad y Derecho Penal”, Bdef, Buenos Aires, 2006.
ALDEGANI, GUSTAVO: “Seguridad informática”. M.P. Ediciones, Buenos Aires, 1997.
ALDEGANI, GUSTAVO: “Virus Informáticos. Conozca a Fondo a Su Enemigo”. M.P. Ediciones, Buenos Aires, 1998.
AREITIO JAVIER: “Seguridad de la Información. Redes Informáticas y Sistemas de Información”. Paraninfo, Madrid, 2008.
BROW, JOHN SEELY y DUGUID, PAUL: “La Vida Social de la Información”. Pearson Education, Buenos Aires, 2001.
CAMPOS ARENAS, AGUSTIN: "Métodos mixtos de investigación, integración de la investigación", Editorial MAGISTERIO, Buenos Aires, 2009.
CANO MARTINEZ, JEIMY: “Computación Forense. Descubriendo los Rastro Informáticos”. Alfaomega Grupo Editor, Madrid, 2009.
CARRANZA TORRES M.- PEREYRA ROZAS M.-BRUERA H.: “Ley de Delitos Informáticos 26.388”, JA 2008- III-647, LEXIS Nº0003/013978.
CEGARRA SANCHEZ, JOSE: "Metodología de la Investigación Científica y Tecnológica", DIAZ DE SANTOS, Madrid, 2004.
COICAUD, SILVIA: "El docente investigador. La investigación y su enseñanza en las universidades", MI\O Y DAVILA, Buenos Aires, 2008.
CREUS, CARLOS: “Derecho Penal Parte Especial”. Editorial Astrea, Buenos Aires, 2002.
DEL PESO NAVARRO, EMILIO: “Peritajes Informáticos”. Ediciones Díaz de Santos S.A, España, 2001.
DREYZIN DE KLOR, ADRIANA, FERNÁNDEZ ARROYO, DIEGO, PIMENTEL, LUIS O: "Internet, comercio electrónico y sociedad de la información ", Zavalia, Buenos Aires, 2004.
FILLIA LEONARDO CESAR-MONTELEONE ROMINA-NAGER HORACIO S. – SUEIRO, CARLOSCHRISTIAN: “Análisis integrado de la Criminalidad Informática”. Prólogo Carlos Alberto Elbert, Editorial Fabian J. di Plácido, Buenos Aires, 2007.
FIRTMAN, SEBASTIÁN: “Seguridad Informática”. M.P. Ediciones, Buenos Aires, 2005.
KNIGHTMARE: “Secretos de un Superhacker”. Juegos & Co SRL, Buenos Aires, 1995.
MCCLURE, SCAMBRAY y KURTZ: “HACKERS. Secretos y Soluciones para la Seguridad de Redes”. McGraw-Hill / Interamericana de España S.A, Madrid, 2000.
MORON LERMA ESTHER: “Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red”, Editorial Aranzandi, Segunda edición, Navarra, 2002.
PALAZZI PABLO: “Los Delitos Informáticos en el Código Penal. Análisis de la Ley 23.688”. Abeledo Perrot, Buenos Aires, 2010.
PICOUTO RAMOS, FERNANDO; GARCIA-MORAN, JEAN PAUL; LORENTE PEREZ, IÑAKI; RAMOS VARON, ANTONIO: “Hacking y Seguridad en Internet”. Alfaomega Grupo Editor, Madrid, 2008.

RIQUERT, MARCELO ALFREDO: "Informática y Derecho Penal Argentina". Editorial Ad-Hoc, 1º Edición, Buenos Aires, 1999.
RIQUERT, MARCELO ALFREDO: "Protección Penal de la intimidad en el espacio virtual", Ediar, Buenos Aires, 2003.

Datos de Contacto:
Betsabé, Lacour: betsy.lacour@gmail.com
Castillo, Noelia: noe_sfe@hotmail.com
Zehnder, Rodolfo: rfzehnder@wilnet.com.ar
Zenobi, Román Pablo: rozenobi@hotmail.com
UCSE - DAR – Departamento Académico Rafaela
O3493-432832. Bv. Irigoyen 1502 (2300) Rafaela, Santa Fe