Sergio Daniel Conde - Osvaldo Donato Marcovecchio - Silvio Ramiro De Cicco
Universidad de la Marina Mercante, Secretaría de Investigaciones Facultad de Ingeniería

La Inseguridad de la Seguridad: Un modelo de aplicación en la Universidad de la Marina Mercante

Abstract

El objetivo de la investigación es demostrar desde el punto de vista del usuario, si los procedimientos de guía para las diferentes contraseñas que se necesitan como cliente de cualquier entidad bancaria hoy en día en Argentina facilitan la gestión de éstas por parte del usuario o todo lo contrario. Se ha propuesto la utilización de una encuesta como herramienta de diagnóstico dirigida a diferentes usuarios de bancos para determinar la opinión de estos sobre las Políticas que deben seguir para gestionar las contraseñas de las diferentes plataformas que ofrecen los bancos para operar. Cabe aclarar que todo esto tiene como objetivo general proteger la información del usuario, haciendo foco en la confidencialidad de la misma sin descuidar su integridad y disponibilidad.
La investigación se realiza en la Universidad de la Marina Mercante en la Ingeniería en Sistemas interviniendo la Asignatura Ingeniería del Software II teniendo especial atención en la Seguridad Informática como parte de los contenidos de las asignatura.
Se parte de la Hipótesis:
Los procedimientos de guía para el cambio de las diferentes contraseñas que se necesitan como cliente de cualquier entidad bancaria hoy en día en Argentina dificultan la gestión.
Se aplica una metodología detallada donde se integran diferentes elementos que permiten identificar el análisis cualitativo y cuantitativo comparando diferentes variables que se encuentran presentes en un determinado ámbito de incumbencia.
Por último para terminar se procede a validar la muestra con los resultados obtenidos.
El tipo de diseño es cuantitativo / cualitativo.

Palabras Clave

Seguridad, Información, Activo de Información, Confidencialidad, Integridad, Disponibilidad, Contraseña, Control, Amenaza, Vulnerabilidad, Riesgo, Impacto, Concientización, Proceso, Procedimiento, Política.

Introducción

Hace relativamente pocos años la Seguridad de la Información era de fácil administración, sólo bastaba con guardar los documentos más importantes bajo llave y brindar protección a los empleados que poseían el conocimiento. Hoy en día esto es mucho más difícil. Con la evolución de los sistemas electrónicos, que han permitido automatizar un sin número de procesos y brindar grandes ventajas por su capacidad de almacenamiento y procesamiento, se han ido constituyendo como un componente fundamental en todas las organizaciones, pero al mismo tiempo se debería desarrollar sistemas que permitan preservar la seguridad de los activos de información y evolucionar conjuntamente para mantenerse al día con la tecnología cambiante. Con la llegada de Internet han surgido los crímenes cibernéticos que causan grandes gastos y pérdidas muy significativas por no mantener Seguridad de la Información.
El objetivo fundamental de la Seguridad de la Información es reducir los riesgos y dar soporte a las operaciones del negocio, pues implementar una solución cien por ciento segura no existe, sólo es posible realizar un proceso de mitigación de riesgos.

El objetivo de la investigación es demostrar Los procedimientos de guía para el cambio de las diferentes contraseñas que se necesitan como cliente de cualquier entidad bancaria hoy en día en Argentina dificultan la gestión.
Se aplica una metodología detallada donde se integran diferentes elementos que permiten identificar el análisis cualitativo y cuantitativo comparando diferentes variables que se encuentran presentes en un determinado ámbito de incumbencia en el momento de realizar cambios en la operatoria de tarjetas electrónicas por internet.
Por último para terminar se procede a validar la muestra con los resultados obtenidos.
El tipo de diseño es cuantitativo / cualitativo.

Elementos del Trabajo y metodología

1. *Marco Teórico*

La Seguridad Informática

La seguridad informática es el área encargada de la protección de las infraestructuras de las Tecnologías de la Información y Comunicación, en adelante TIC. Por ejemplo: en seguridad informática, podemos implementar algunos controles para la protección del equipamiento informático y de los sistemas de información contra ataques o códigos maliciosos, como Antivirus y Corta Fuegos (Firewall).
En cambio, la seguridad de la información es el área encargada de la protección de los activos de información en cuanto a las siguientes propiedades de la información: confidencialidad, integridad, disponibilidad, autenticidad, no repudio, trazabilidad. Como la información puede estar contenida en diferentes soportes, medios, formas y no sólo en medios informáticos, aquí podemos citar como ejemplos documentación en papel, mobiliarios con diferentes documentos en su interior, y el recurso humano que es el activo de información más importante dentro de las organizaciones.
En síntesis, la seguridad de la información abarca la seguridad informática.

Figura 1: Grafico que comprende la seguridad informática.

Activo de información

Un activo de información, es todo aquello que tiene un valor para la organización, pero que al mismo tiempo almacena y manipula información. Por ejemplo, una cajonera con expedientes en su interior, debe ser considerado un activo de información y, como tal, debe protegerse. En cambio una cajonera vacía, no representa un activo de información para la organización, sino un bien de uso. Es fundamental tener en claro este concepto para darles la protección adecuada a estos activos.
La información posee ciertas propiedades que definiremos a continuación:

- confidencialidad: es la propiedad de la información por la que se garantiza que sólo esta accesible por el personal autorizado.
- integridad: es la propiedad de la información por la que se garantiza que la misma no ha sido alterada.
- disponibilidad: es la propiedad de la información por la que se garantiza que está disponible siempre y cuando se la requiera.
- autenticidad: es la propiedad de la información por la que se garantiza la veracidad y exactitud de la misma.
- no repudio: es la propiedad de la Información por la que se garantiza la autoría de la misma.
- trazabilidad: es la propiedad de la información por la que se garantiza quién hizo qué y cuándo lo hizo.

Estos conceptos son fundamentales a la hora de identificar nuestros activos de información y realizar un análisis con respecto a todas sus propiedades, para decidir el nivel de protección adecuado que se necesita.
Los activos de información se deben inventariar en un documento llamado Inventario de activos de información. Para que este último sea transparente y entendible se pueden discriminar en diferentes categorías. Por ejemplo:

- Datos: todos aquellos datos que, en cualquier formato, se generan, se recogen, se gestionan, se transmiten y se destruyen.
- Aplicaciones: el producto de software que se utiliza para gestionar la información.
- Personal: todos aquellos que tengan acceso de una u otra forma a los activos de información.
- Servicios: servicios internos como externos.
- Tecnología: los equipos que se utilizan para gestionar la información y las comunicaciones.

Equipamiento Auxiliar: son aquellos activos que dan soporte a los sistemas de información y que no están incluidos en ninguna de las categorías anteriores. Ejemplos de esto último son equipos de destrucción de datos, equipos de climatización, etc.

Fallo en la Seguridad.

Un fallo de seguridad es cualquier incidente que la compromete, es decir que pone en peligro cualquiera de las propiedades de la información descriptas anteriormente. Como ejemplo de fallo de seguridad, podemos citar: fallos en el suministro eléctrico, fallos en las comunicaciones, fallos humanos (ya sean internos como externos a la organización), fallos en los sistemas de información, códigos maliciosos,

accesos no autorizados o incumplimiento de leyes o reglamentos.
Los fallos de seguridad a menudo suceden porque se tiene la errónea percepción de que si la seguridad física está asegurada no debería haber mayores inconvenientes. O porque tenemos asegurado todo lo referente a la seguridad informática. Pero de esta manera se deja sin protección muchas áreas y muchos activos de información pueden ser dañados o destruidos por no considerar todos los aspectos de seguridad de la información.
Para entender un poco más este punto debemos saber que existen amenazas potenciales, que pueden explotar vulnerabilidades de nuestros activos de información produciendo riesgos, y de esta forma tendremos un impacto determinado sobre nuestro negocio. A continuación describiremos los criterios de la información sobre estos puntos:

- Amenaza: evento que puede comprometer un activo de información.
- Vulnerabilidad: debilidad que hace susceptible a un activo de información.
- Riesgo Intrínseco: nivel de riesgo sin ningún tipo de control aplicado al mismo.
- Riesgo Residual: nivel de riesgo resultante una vez aplicados los controles.
- Impacto: resultado de la materialización de la amenaza.
- Proceso
  Tratamiento determinado que resulta de la aplicación de diferentes procedimientos.
- Procedimiento

Conjunto de instrucciones técnicas que llevan a un tratamiento determinado (Proceso).

- Política

Es lo que busca y entiende cualquier persona, física o jurídica, por seguridad de la información. Acá influye mucho la cultura organizacional y personal según corresponda.

- Autenticidad

Es la propiedad de la información por la que se garantiza la veracidad y exactitud de la misma.

- No Repudio

Es la propiedad de la Información por la que se garantiza la autoría de la misma.

- Trazabilidad

Es la propiedad de la información por la que se garantiza quién hizo qué y cuándo lo hizo.

Marco Legal

Ley de Protección de Datos Personales N° 25.326
Artículo 17: Seguridad.
Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

- El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente reglamento, identificar sus deficiencias y proponer las medidas correctoras y complementarias necesarias. Deberá, incluir datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.
- Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

Tipos de ficheros.

- Todos los ficheros que contengan datos de carácter personal.
- Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, etc.
- Los ficheros que contenga datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas.
- Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.

Ley N° 24.766.- Confidencialidad
Ley N° 25.036.- Modificatoria de la
Ley N° 11.723.- Propiedad Intelectual
Ley N° 25.188.- Ética en el ejercicio de la función pública
Ley N° 25.506.- Firma Digital
Ley N° 25.520.- Inteligencia Nacional
Ley N° 26.388.- Delitos Informáticos. Modificación al Código Penal
Decisión Administrativa 669/04. Políticas de seguridad de la información

Estándares

ISO/IEC 27000: SGSI. Conceptos y generalidades
ISO/IEC 27001: SGSI. Requisitos
ISO/IEC 27002: Código de buenas prácticas para la gestión de la seguridad de la información
ISO/IEC 27003: Guía de implementación de un SGSI. Circulo de Deming o PDCA (Planificar, Hacer, Checkear, Actuar). Ciclo de mejora continua.
ISO 27004: Métricas. Medición efectividad controles.
ISO/IEC 27005: Metodología para la Gestión del Riesgo
ISO/IEC 27006: Requisitos para entidades de servicio de Auditoría y Certificación de SGSI
ISO/IEC 27007: Guía para la realización de Auditorías de un SGSI
ISO/IEC 27011: Directrices para la seguridad de la información en organizaciones de Telecomunicaciones utilizando la Norma ISO/IEC 27002
ISO/IEC 27799: Gestión de la seguridad de la información sanitaria utilizando la Norma ISO/IEC 27002
La Norma ISO/IEC 27001 es la única certificable de la serie.

Amenazas más comunes de un acceso no autorizado.

- Ingeniería Social

- Keylogger
- Spyware
- Cookies Maliciosas
- Ataques a nivel red
- Botnets
- Phishing
- Pharming [1].

La sociedad red

Castells M, define a la sociedad red como un conjunto de nodos Interconectados con capacidad de expansión ilimitada entre los que compartan unos mismos códigos. Se van creando distintos tipos de redes a partir de las cuales la sociedad se estructura y la comunicación entre los puntos interconectados de una red fluye sin que exista distancia - tiempo entre ellos. La conexión entre elementos ajenos a una misma red viene marcada por distancias inexistentes en el caso anterior. De esta forma, las relaciones en la sociedad quedan marcadas por la inclusión o exclusión de las redes. [2].

1.3 *La protección de datos*

La ley 1845/2006 de protección de datos personales establece Definiciones. A los fines de la presente ley se entiende por:

Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal, determinada o determinable.

Datos sensibles: Aquellos datos personales que revelan origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o cualquier otro dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio al titular de los datos.

Archivos, registros, bases o bancos de datos: Indistintamente, designan al conjunto organizado de datos personales objeto de tratamiento, cualquiera sea la modalidad o forma de su recolección, almacenamiento, organización o acceso, incluyendo tanto los automatizados como los manuales.

Tratamiento de datos: Cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, registro, organización, elaboración, extracción, utilización, cotejo, supresión, y en general, el procesamiento de datos personales, así como también su cesión a terceros a través de todo tipo de comunicación, consulta, interconexión, transferencia, difusión, o cualquier otro medio que permita el acceso a los mismos.

Titular de datos: Persona física o de existencia ideal cuyos datos sean objeto de tratamiento.

Responsable del archivo, registro, base o banco de datos: Persona física o de existencia ideal del sector público de la Ciudad de Buenos Aires que sea titular de un archivo, registro, base o banco de datos.

Encargado del tratamiento: Persona física o de existencia ideal, autoridad pública, dependencia u organismo que, solo o juntamente con otros, realice tratamientos de datos personales por cuenta del responsable del archivo, registro, base o banco de datos.

Usuario de datos: Persona física que, en ocasión del trabajo y cumpliendo sus tareas específicas, tenga acceso a los datos personales incluidos en cualquier archivo, registro, base o banco de datos del sector público de la Ciudad de Buenos Aires.

Fuentes de acceso público irrestricto: Exclusivamente, se entienden por tales a los boletines, diarios o repertorios oficiales, los medios de comunicación escritos, las guías telefónicas en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección o cualquier otro dato que indique de su pertenencia al grupo. [3]

Padilla define al derecho a la intimidad "como el derecho que tienen los individuos, los grupos y las instituciones, de determinar por su cuenta cómo y en qué medida las informaciones que les atañen pueden ser recolectadas, tratadas y, eventualmente, comunicadas a otras personas". [4]

El avance de las nuevas tecnologías ha facilitado enormemente la recolección y almacenamiento de los datos personales. La computadora y el uso de Internet posibilitan el rápido y completo tratamiento de datos personales. Se habla así actualmente del derecho a la "autodeterminación informativa" como la facultad que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente los almacenados mediante medios informáticos. [5]

Bidart Campos señala "en la autodeterminación informativa aparece una fase activa que, en el proceso de circulación de la información personal, confiere al interesado un protagonismo fuerte para intervenir con fines de control y preservación de sus datos, en todo lo que en cuanto a su veracidad y confidencialidad le conciernen".

1 Conde Sergio D. y Marcovecchio Osvaldo (2015). *El Conocimiento Organizacional*. Argentina. Editorial Aplicación.

2 Conde, Sergio D y De Cicco Silvio (2014). *La Comunicación Tecnológica*. Argentina. Editorial Aplicación.

3 Ley CABA N°: 1845 / 2006. Publicado en el B.O. CABA N° 2494 el 03-08-2006.

4 Padilla, Miguel M. *Bancos de Datos y Acción de Hábeas Data* Editorial Abeledo Perrot – Buenos Aires – pág. 31

5 Viggiola Lidia. y Molina Quiroga, Eduardo. En su trabajo: "*Tutela de la autodeterminación informativa. Aproximación a una regulación eficaz del tratamiento de datos personales*". Ponencia presentada al Congreso Internacional "Derechos y Garantías en el Siglo XXI" de la Asociación de Abogados de Buenos Aires.

Pero dentro de los datos que hacen a la intimidad existen datos íntimos y totalmente privados de las personas, cuya divulgación afecta de manera particular no solo a su intimidad sino también a su privacidad. [6]

Miguel S. Elías interpreta a los datos sensibles "como aquellos que por sí solos impulsan naturalmente a un individuo a la más íntima y absoluta reserva de dicha información". [7]

Por su parte Carlos Paladella Salord asume una postura en relación a los datos personales íntimos: "Se trata de información relativa al fuero interno de las personas, es decir, que identifica los sentimientos, la personalidad, las creencias y pensamientos de orden privado de las personas. Se trata de partes del ser que se revelan exclusivamente de forma particular e individual, y rara vez son objeto de tratamiento público" [8]

Horacio M. Lynch y Mauricio Devoto sostienen "En las primeras épocas de estudio de los datos personales se discriminó entre los datos comunes y los llamados sensibles, precisamente porque afectaban con particular incidencia la esfera personal del individuo o persona. Anticipamos ya que en un trabajo publicado en 1996 expresamos la idea de que esta clasificación había perdido importancia, desde que la sumatoria de datos no sensibles podía revelar, mediante los recursos utilizados, datos sensibles, inclinaciones o tendencias" [9]

2. *Desarrollo*

Para desarrollar la investigación se elabora una encuesta que es contestada por 100 (cien) personas donde se solicita responder:

1) Tiene más de una cuenta que opere con contraseñas
   Incluye tarjetas, cuentas bancarias, home banking y cuentas de internet
   Hasta tres.
   Entre tres y cinco.
   Más de cinco.
   No tengo tarjetas.
2) Debes cambiar las contraseñas en forma obligatoria
   En todas.
   En algunas.
   No es obligatorio cambiar contraseña
3) Con qué Frecuencia cambias las contraseñas
   Mensualmente.
   Trimestralmente.
   Anualmente.
   No cambio contraseñas.
4) Debes colocar una cantidad de caracteres en forma obligatoria
   Mínima.
   Exacta.
5) Los caracteres deben incluir
   Sin condiciones.
   Mayúsculas y Minúsculas.
   Mayúsculas, Minúsculas y números.
6) La cuenta que le exige el cambio de contraseña permite:
   Utilizar los mismos caracteres en otro orden.
   Cambiar algún carácter de la contraseña vieja.
   Cambiar más de tres caracteres de contraseña vieja.
   Cambiar radicalmente la contraseña
7) El procedimiento de cambiar la contraseña le produce dificultad para recordar la nueva contraseña
   Si
   No
8) Este procedimiento lo obliga a utilizar una muletilla para acordarse de su contraseña
   Si
   No
9) Considera que el procedimiento de cambiar contraseña le da más seguridad a sus datos
   Si
   No
10) De los siguientes elementos cuales considera que perjudican
    Cambio de contraseña complicado
    Demora en el tiempo de cambiar la contraseña
    Ninguna de las opciones

Procesando la Información

Gráfico 1: Gráfico de Cantidad de tarjetas que tiene una persona.

Se observa que 37 (treinta y siete) personas tienen entre tres y cinco tarjetas con un porcentaje del 37%.

37 (treinta y siete) personas tienen hasta tarjetas con un porcentaje del 37%.

26 (veintiseis) personas tienen hasta tarjetas con un porcentaje del 26%.

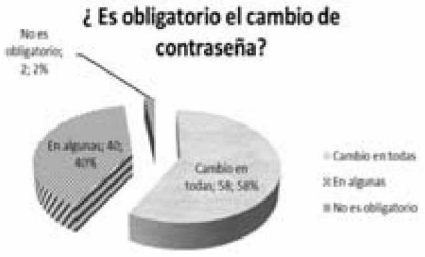

Gráfico 2: Gráfico de cambio de contraseña.

6 Bidart Campos, German -"*Tratado Elemental de Derecho Constitucional Argentino*", Edición 2000-2001 Tomo I-B, Edit. Ediar, pág. 69.

7 Elias, Miguel Sumer - "*Situación Legal de los Datos de carácter Personal frente a las Nuevas Tecnologías*". Ponencia presentada en el Congreso Internacional por Internet sobre Aspectos Jurídicos del Comercio Electrónico – ECOMDER- celebrado en Buenos Aires durante el año 2001.

8 Paladella Salord, Carlos "*Datos Personales Contenidos en Bases de Datos y Registro Electrónicos*" http://www.it-cenit.org.ar/Publicac

9 Lymch, Horacio M. y Devoto, Mauricio - *Bases de datos electrónicos y el Habeas Data –Problemática legal–* Investigación CENIT # 1/98 - http://www.it-cenit.org.ar/Publicac

Se observa que es obligatorio el cambio de contraseñas en 58 (cincuenta y ocho) personas con un porcentaje del 58%.
En algunas tarjetas permite el cambio de contraseñas en 40 (cuarenta) personas con un porcentaje del 40% y 2 (dos) personas no tienen la obligación de cambiar contraseñas con un porcentaje del 2%.

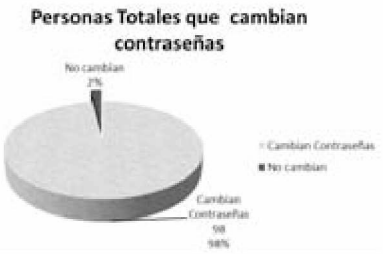

Gráfico 3: Gráfico d Personas Totales que cambian de contraseña.

Analizando los resultados del último gráfico se observa que 98(noventa y ocho) personas tienen la obligación de cambiar contraseñas con un porcentaje de 98% y 2 (dos) personas no cambian contraseñas con un porcentaje del 2%.

Gráfico 4: Gráfico Tiempo de Cambio de contraseñas.

Se observa que cambian contraseñas trimestralmente 60 (sesenta personas) con un porcentaje del 60%.
Cambian contraseñas mensualmente 35 (treinta y cinco) personas con un porcentaje del 35%.
Cambian anualmente contraseñas 5 (cinco) personas con un porcentaje del 5%.

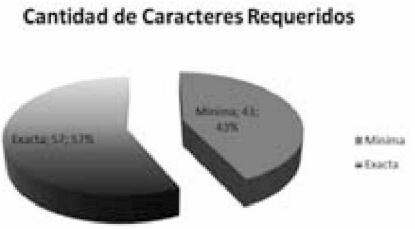

Gráfico 5: Gráfico de Caracteres Requeridos.

Se observa que piden cambiar exactamente los caracteres de la contraseña a 57 (cincuenta y siete) personas con un porentaje del 57%
Piden cambiar una cantidad mínima de los caracteres de la contraseña a 43 (cuarenta y tres) personas con un porentaje del 43%.

Gráfico 6: Gráfico de Característica de la Contraseña.

Se observa que 87 (ochenta y siete) personas le pide cambiar mayúsculas, minúsculas y números con un porcentaje del 87%.
Se observa que 10 (diez) personas le pide cambiar minisculas y números con un porcentaje del 10%.
Se observa que 3 (tres) personas no tienen condicones de cambio especificado con un porcentaje del 3%.

Gráfico 7: Gráfico de Estadística Total de Formato de Contraseñas.

Se observa que 97 (noventa y siete) personas tienen que respetar un formato específico con un porcentaje del 97% y 3 (tres) personas no tienen que respetar un formato específico con un porcentaje del 3%.

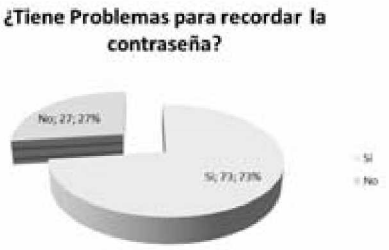

Gráfico 8: Gráfico de Recuerdo de Contraseña.

Se observa que 73 (setenta y tres) personas tienen problemas para recordar contraseñas con un porcentaje del 73% y 27 (veintisiete) personas no tienen problemas en recordar la contraseña con un porcentaje del 27%.

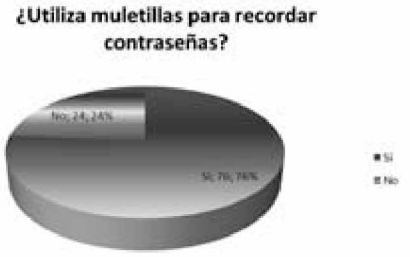

Gráfico 9: Gráfico de utilización de muletillas.

Se observa que 76 (setenta y seis) personas usan muletillas con un porcentaje del 76% y 24 (veinticuatro) personas no utilizan muletillas para recordar la contraseña con un porcentaje del 24%.

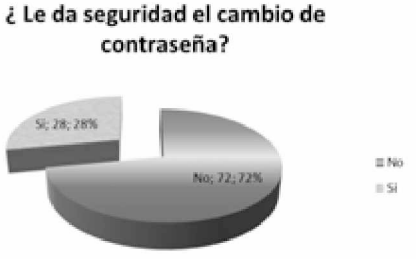

Gráfico 10: Gráfico de seguridad en el cambio de contraseña.

Se observa que 72 (setenta y dos) personas no le da seguridad el cambio de contraseña con un porcentaje del 72% y 28 (veintiocho) personas le da seguridad el cambio de la contraseña con un porcentaje del 28%.

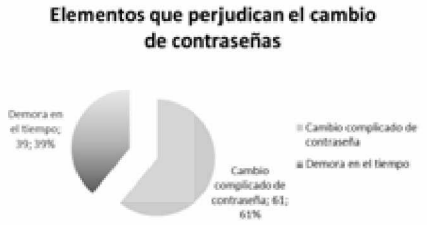

Gráfico 11: Gráfico elementos que perjudican el cambio de contraseña.

Se analiza que 61 (sesenta y una) personas consideran que es complicado el cambio de contraseñas con un porcentaje del 61% y 39 (treinta y nueve) personas consideran que es una demora en el tiempo el cambio de contraseñas con un porcentaje del 39%.

Gráfico 12: Gráfico Características de la nueva contraseña.

Se analiza que 50 (cincuenta) personas deben cambiar en forma total la contraseña con un porcentaje del 50%.
27 (veintisiete) personas deben cambiar algún carácter con un porcentaje del 27% y 23 (veintitres) personas deben cambiar más de tres caracteres con un porcentaje del 23%.

Validando Resultados

Estadísticas	SI	NO
Usa Muletillas	76	24
Seguridad Cambio de Contraseña	72	28
Problemas para Recordar Contraseñas	73	27
Cambio con Formato Específico de Contraseña	97	3
Personas que cambian Contraseñas	98	2
Media	83,20	16,80
Desviación Estándar	13,14	13,14
Desviación Estándar / Media	0,16	0,78

Tabla 1: Tabla de Estadística de validación de muestra.

Analizando el total de las personas que contestaron afirmativamente y que tienen inconvenientes en la complejidad del funcionamiento del sistema en el cambio de claves se obtiene una validación de 0,16 en respuestas afirmativas con una validación de 0,78 en respuestas negativas.

Gráfico 13: Gráfico Validación de la muestra.

Conclusión.

Se puede verificar que la hipotesis planteada: Los procedimientos de guía para el cambio de las diferentes contraseñas que se necesitan como cliente de cualquier entidad bancaria hoy en día en Argentina dificultan la gestión.
es validada.
Se puede identificar que 73(setenta y tres) personas tienen problemas en recordar contraseñas debiendo utilizar 76(setenta y seis) personas muletillas y 72 personas el hecho de cambiar contraseñas no le da seguridad en el ambiente que se desenvuelve.
Atribuyen las causas a que necesitan un formato específico 97 (noventa y siete) personas.
Consideran que es complicado el cambio de contraseña 61 (sesenta y uno) personas y 39 (treinta y nueve) personas consideran que es perdida de tiempo.
60 (sesenta) personas cambian trimestralmente las contraseñas siendo contraproducente para recordar las mismas.
35 (treinta y cinco) personas cambian mensualmente las contraseñas siendo contraproducente para recordar las mismas.
Teniendo en cuenta cuando Padilla define al derecho a la intimidad "como el derecho que tienen los individuos, los grupos y las instituciones, de determinar por su cuenta cómo y en que medida las informaciones que les atañen pueden ser recolectadas, tratadas y, eventualmente, comunicadas a otras personas" se observa que el estar expuestos en el cambio de contraseñas en un período de tiempo se pierde intimidad y se gana como contrapartida inseguridad.
Teniendo en cuenta la expresión de Viggiola, Lidia E. y Molina Quiroga El ordenador y el uso de Internet posibilitan el rápido y completo tratamiento de datos personales. Se habla así actualmente del derecho a la "autodeterminación informativa" como la facultad de toda persona para ejercer control sobre la información personal

que le concierne, contenida en registros públicos o privados, especialmente los almacenados mediante medios informáticos se puede determinar que la persona se encuentra expuesta a el inadecuado control de la información que es controlada por un servidor y esta a disposición del robo del activo como un elemento fundamental.

Teniendo en cuenta a Bidart Campos cuando afirma que dentro de los datos que hacen a la intimidad existen datos íntimos y totalmente privados de las personas, cuya divulgación afecta de manera particular no solo a su intimidad sino también a su privacidad se puede afirmar que las personas que cambian contraseñas con la complejidad establecida en la muestra pierden la intimidad y privacidad de los datos obligados a cambiarlos en un periodo de tiempo determinado.

Fortalezas:

- Se puede determinar la validación comprobable de la muestra.
- Identificar elementos que provocan inseguridad.
- Optimizar la evaluación de todos los elementos que provocan inseguridad.

Debilidades:

- El resultado del análisis cualitativo y cuantitativo obtenido en las respuestas de la muestra junto con el Análisis de Desviación permite puede observar que los elementos críticos que se aplican en el control y aplicación de contraseñas.
- Permite integrar la aplicación de competencias de conceptos teóricos de Seguridad Informática y Normas de Calidad que se contemplan en el diseño curricular de la Asignatura por intermedio de la investigación.