



# MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

## **Validación del Instrumento Self Report Habit Index (SRHI) para medir la fuerza del hábito en el uso de los sistemas de información en el sector hospitalario.**

Propuesta de artículo presentado como requisito para la obtención del título:

### **Magíster en Auditoría de Tecnologías de la Información**

Por los estudiantes:

**Gustavo Mauricio VELEZ DROUET.  
Juan Antonio GALAN ABRIL.**

Bajo la dirección de:

**Francisco Josep BOLAÑOS BURGOS.**

Universidad Espíritu Santo  
Maestría en Auditoría de Tecnología de la Información  
Samborondón - Ecuador  
Marzo del 2019

## Validación del Instrumento Self Report Habit Index (SRHI) para medir la fuerza del hábito en el uso de los sistemas de información en el sector hospitalario.

Validation of the Self Report Habit Index Instrument (SRHI) to measure the strength of habit in the use of information systems in the hospital sector.

**Gustavo Mauricio VELEZ DROUET<sup>1</sup>**  
**Juan Antonio GALAN ABRIL<sup>2</sup>**  
**Francisco Joseph BOLAÑOS**  
**BURGOS<sup>3</sup>**

\*

### Resumen

El presente estudio tiene como objetivo validar la teoría del índice de Hábito de Auto informe para medir la fuerza del hábito de una institución pública en el sector hospitalario, se diseñaron 3 escenarios relacionados con las primeras 3 políticas de seguridad de la información más relevantes en el hospital. Los ítems fueron evaluados con una escala Likert de 5 categorías: (1) nunca, (2) casi nunca, (3) a veces, (4) casi siempre y (5) siempre. El análisis de los resultados se procedió mediante las correlaciones de los ítems asociados con la frecuencia y automaticidad en cada escenario con una muestra de 70 funcionarios médicos de diferentes especialidades. Los resultados muestran una probabilidad mayor o igual 0.50 en los 12 ítems demostrando un alto nivel de fiabilidad y validez del SRHI para medir hábitos de compartir sus contraseñas de acceso a los sistemas de información en los funcionarios, evidenciado en las políticas más relevantes.

**Palabras clave:** Hábito, frecuencia, automaticidad, SRHI, señal de contexto

### Abstract

The objective of this study is to validate the Self Report Habit Index to measure the strength of a public institution's habit in the hospital sector, 3 scenarios were developed in relation with the first 3 most relevant information security policies in the hospital. The items were evaluated with a Likert scale of 5 categories: (1) never, (2) almost never, (3) sometimes, (4) almost always, and (5) always. The analysis of the results was carried out by means of the correlations of the items associated with the frequency and automaticity in each scenario with a sample of 70 medical officers from different specialties. The results show a probability greater than or equal to 0.50 in the 12 items demonstrating a high level of reliability and validity of the SRHI to measure habits of sharing their passwords of access to the information systems in the officials, evidenced in the most relevant policies

**Key Word** Habit, frequency, automatacity, SRHI, cue

---

<sup>1</sup> Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail [gvelezd@uees.edu.ec](mailto:gvelezd@uees.edu.ec)

<sup>2</sup> Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail [igalana@uees.edu.ec](mailto:igalana@uees.edu.ec)

<sup>3</sup> Magíster en Seguridad Informática Aplicada. Director de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo- Ecuador.

## INTRODUCCIÓN

La implementación y ejecución de las políticas de seguridad de los sistemas de información (SI), es un desafío que ha ido tomando importancia dentro de organizaciones tanto gubernamentales como privadas, debido al gran reto al que se enfrentan hoy en día, el concientizar a los empleados a cumplir con todas las normas de seguridad (Aytes, 2004).

Se consideran los diferentes comportamientos de las personas en cuanto a estas políticas, en las que pueden reaccionar de una u otra manera dependiendo de sus constructos sociales como: la intención, la cual se puede generar a través de deliberaciones reflexivas o procesos superficiales (Armitage, 2004). Así también los hábitos se manifiestan como respuestas de comportamiento aprendidas a señales situacionales que se han establecido en la tradición conductista como lo demuestra Hull (1943), a través de una historia de repetición y refuerzo sistemático, por lo tanto, la intención del usuario frente a la utilización de ciertas medidas de seguridad dentro de una empresa depende muchas veces del hábito que haya concebido.

Se infieren estudios enfocados en el comportamiento habitual que desearan los empleados en cuanto al manejo de dichas políticas de seguridad, transformándose en automáticos, que se desencadena por las señales situacionales y puede ejecutarse con poca conciencia (Aytes, 2003).

De la misma manera, al utilizar un procedimiento diario de señal-contingente, como lo sugirió (Wood, Jeffrey, & Kashy, 2002), se pudo manifestar la alta probabilidad en que las personas seleccionadas para el estudio etiquetaron sus acciones como habituales.

Por lo tanto, una característica importante de los hábitos es la automaticidad de las actividades, según Aarts y Dijksterhuis (2000). Por otro lado, Bargh (1994) sugirió que la automaticidad se puede dividir en una serie de características como: eficiencia mental; falta de conciencia, control y falta de intención consciente.

Dentro del contexto local no se encuentran muchos estudios realizados sobre el hábito y lo que se puede encontrar son estudios realizados a nivel general, que tratan sobre los diferentes hábitos en cuanto a la aplicación de las políticas de seguridad, como las investigaciones de Charng et al. (1988), que manifiesta que un hábito se desarrolla por la repetición a menudo de cierta actividad, concepto que comparte con Kim (2005) y Limayem (2007), quienes ponen como

condición previa para el desarrollo del hábito, la repetición constante de dicha actividad.

En consecuencia, cuanto más a menudo uno realiza el comportamiento, es más probable que el comportamiento se convierta en un hábito, según manifiesta Charng (1988); por lo tanto, el hábito se debe impulsar en los usuarios desde su práctica voluntaria y repetitiva, no como una necesidad sino más bien como una obligación, que permita un mejor y fiel cumplimiento de la Política de seguridad de la información (PSI), en la que según (Siponen M. T., 2000) se debe al cambio de comportamiento de manera intencional o no intencional, situación que ha sido examinada a través de revisiones sistemáticas y meta análisis, donde se proponen doce teorías, de las cuales, las más utilizadas son: Teoría general de la disuasión (GDT), Teoría del Comportamiento Planificado (TPB), Teoría de la motivación de la protección (PMT) y la Teoría del índice de auto informe del hábito (SRHI).

La Teoría del índice de autoinforme del hábito (SRHI) aplicado en más de 300 estudios empíricos en muchos contextos mide distintas facetas de una repuesta repetida y por lo tanto no sólo se basa en la frecuencia del comportamiento, también evalúa la fuerza cognitiva, (Verplanken & Sheina, 2015). Así como también puede detectar asociaciones hábito-comportamiento, moderación en las relaciones intencion-comportamiento (Gardner, Abraham, Lally, & de Bruijn, 2012).

El presente estudio tiene como objetivo validar la teoría del índice de auto informe del hábito a través de análisis estadístico correlacionando cada ítem, en relación con las políticas de seguridad de los sistemas de información más relevantes aplicado en una institución pública del sector hospitalario donde se reserva y almacena gran cantidad de información.

## MARCO TEÓRICO

### Hábito

Es un proceso por el cual una señal o estímulo genera un impulso hacia la acción mediante asociaciones estímulo-respuesta aprendidas (Gardner, 2015), el comportamiento es repetido en entornos estables hasta que se convierte en automático sin propósito de pensamiento y en la mayoría de las veces sin sentido de la conciencia (Lally & Gardner, 2013).

Diferentes definiciones de hábito coinciden con la idea de que tres aspectos son fundamentales: un hábito es frecuentemente basado en la repetición, tiene un alto grado de automaticidad y es señalado en contextos estables (Verplanken & Orbell, 2010).

## Repetición

La mayoría de las acciones que se ejecutan diariamente son caracterizadas por la repetición, aproximadamente el 45% de estas acciones se repiten en un mismo entorno cada día (Neal, Wood, & Quinn, 2006). Cuando el comportamiento ha sido suficientemente repetido este puede convertirse en un hábito, en el cual resulta de la automaticidad en responder a señales específicas en el entorno (Verplanken & Orbell, 2003).

## Automaticidad

Son las respuestas automáticas aprendidas con características específicas como pensamiento limitado esto quiere decir que los hábitos son activados en memoria de forma involuntaria sin control cognitivo (Wood & Runger, 2016). Otra característica es rapidez y eficiencia de tal manera que se requiere poco esfuerzo mental para ejecutar una acción, existe fluidez de comportamiento (Verplanken & Aarts, 1999).

La automaticidad se define como el ingrediente activo del hábito debido a que es disparado automáticamente y frecuentemente, anula la motivación cuando es realizado en similares contextos (Gardner, Abraham, Phillipa, & de Bruijn, 2011).

## Señales de Contexto

Las señales de contexto son los factores del entorno de desempeño que fuertemente reinciden a medida que se repiten las acciones, estos factores pueden ser: tiempo, lugar, persona o grupo de personas y secuencia de acciones. Una variedad de respuestas pueden ser preparadas por un conjunto de señales que en el pasado se relacionaron con la respuesta (Neal & Wood, 2007).

Los hábitos se desarrollan en contextos estables, el comportamiento se forma mediante la adquisición de asociaciones entre señales del contexto, respuestas de las personas y consecuencias experimentadas, por lo tanto, una persona debe encontrar situaciones que son similares con respecto a las señales, respuestas y consecuencias (Verplanken & Aarts, 1999).

## Formación del Hábito

De acuerdo a la neurociencia cognitiva cuando un comportamiento es realizado por primera vez es decir de forma no habitual, esta actividad es controlada por el sistema cerebral alojado en la corteza prefrontal (sistema objetivo) diseñado para controlar el comportamiento mediante atención deliberada y altamente involucrado en el

aprendizaje consciente de esfuerzo para nuevos comportamientos (Poldrack, Clark, Blagoev, Shohamy, Moyano, Myers & Gluck, 2001).

Una vez que el comportamiento es repetido, un distinto sistema cerebral toma control del comportamiento, principalmente controlado por los ganglios basales responsables de comportamientos frecuentes y establecidos en un mismo contexto (Neal, Wood, Wu, & Kurlander, 2011).

Este sistema conocido como el sistema del hábito aprende progresivamente a través del tiempo y la repetición, una secuencia de acción debe activar la ejecución automática de una determinada respuesta. Cuando estas asociaciones señal-respuesta han sido formadas y almacenadas en memoria ya no es necesario la participación de la corteza prefrontal con su esfuerzo, atención y motivación. Esta transición desde el sistema objetivo hacia el sistema del hábito ocurre espontáneamente sin que las personas necesariamente sean conscientes o se enteren de que el comportamiento se convirtió en habitual (Neal, Vujcic, Hernandez, & Wood, 2015).

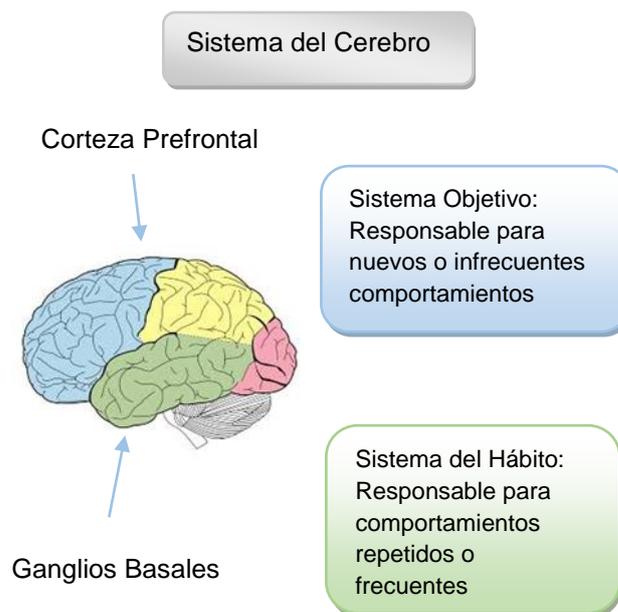


Figura 1: Sistema del Cerebro  
Fuente: (Neal, Vujcic, Hernandez, & Wood, 2015)

## Hábito en la Intención

Las intenciones son los factores motivacionales que influyen en el comportamiento como indicaciones de lo fuerte que las personas están dispuestas a hacer el intento y el esfuerzo que se planea invertir con el fin de realizar el comportamiento (Ajzen, 1991).

Cuando las intenciones de las personas están guiadas con el comportamiento habitual es factible que sus acciones sean automáticas y

señaladas directamente por el contexto. Cuando las intenciones van en sentido opuesto al comportamiento habitual, es probable que las respuestas sean conducidas por las intenciones siempre y cuando sean demasiado fuertes como para anular el comportamiento habitual (Oullette & Wood, 1998).

Por su parte Wood, Jeffrey, & Kashy (2002) definen que el comportamiento pasado es el primer predictor del comportamiento futuro cuando las acciones han sido desarrollados de forma frecuente y en contextos estables (hábito), mientras que las intenciones son el primer predictor del comportamiento futuro cuando las acciones son relativamente nuevas o ejecutadas en contextos distintos.

Gardner (2015) establece dos caminos para llegar hacia el comportamiento, uno es conocido como el camino reflexivo guiado por la intención ejecutado en entornos difíciles o diferentes y poco frecuentes en el cual se requiere capacidad de pensamiento. El otro camino es considerado como el camino impulsivo en el cual se requiere un mínimo de pensamiento, ejecutado en entornos similares y frecuentes guiados por el hábito.

### Hábito en el Pensamiento

En estudios ilustrados por Wood, Jeffrey, & Kashy (2002) representan de mejor manera la relación entre hábito y pensamiento, conducido a estudiantes de la Universidad de Texas reportando a través de encuestas en línea las actividades diarias por cada hora con sus pensamientos y emociones asociados con sus comportamientos habituales y no habituales. Cuando los estudiantes estaban comprometidos con su comportamiento habitual, los pensamientos estaban guiados a problemas no relacionados con su comportamiento y por el contrario, cuando los estudiantes comprometidos con su desempeño no habitual sus pensamientos si estaban relacionados con su comportamiento, esto demuestra que el pensamiento fue necesario para guiar la acción y que el desempeño frecuente del acto y la estabilidad de contexto puede reducir la cantidad de pensamiento necesario para la acción.

### Hábito en la Actitud

Para Fazio (1990) se distinguen dos formas por las cuales las actitudes pueden guiar el comportamiento, de manera deliberada y por la ruta espontánea, las actitudes pueden relacionarse con los hábitos a través de la ruta espontánea, si las actitudes y los hábitos están relacionados, esto será en la medida en que las actitudes sean accesibles en memoria.

El hábito es conducido a procesar menos información cuando un comportamiento es formado, las personas asocian situaciones comparables con ese mismo comportamiento, mientras que la actitud gestiona la información en mayor detalle. Esto significa que cuando el hábito es fuerte la relación actitud-comportamiento es débil y cuando el hábito es débil la relación actitud-comportamiento es fuerte (Verplanken & Aarts, 1999).

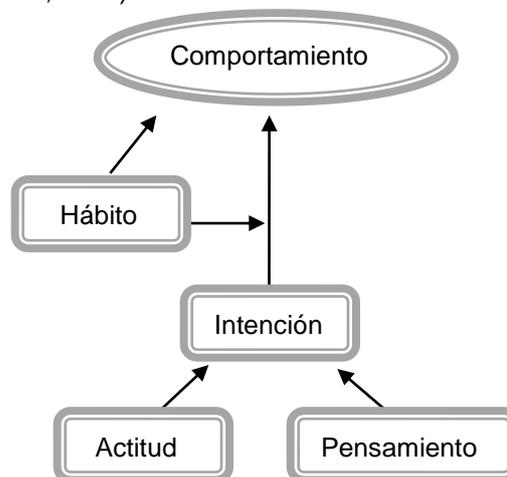


Figura 2: Hábito-Intención-Actitud-Pensamiento. Fuente (Gardner, 2015)

### Medición de la Fuerza del Hábito

Se reconoce generalmente a la fuerza del hábito como el incremento en la medida de que un acto se ha repetido, la fuerza de los hábitos en la vida diaria se evalúan a partir de los auto-informes de las personas (Wood & Runger, 2016).

Si bien es cierto dicha medición de preguntar a las personas para informar sobre sus percepciones del hábito con un solo ítem de autoinforme de hábito típicamente empleado no tenía validez, la formulación de escalas de múltiples ítems enfocados a varios aspectos del hábito y evaluados de diferentes formas pueden generar mayor valor para la medición de la fuerza del hábito (Verplanken & Aarts, 1999). Sin embargo si se mide adecuadamente es probable que las personas sean conscientes de su comportamiento en el grado en que es habitual y debería de requerirse dos condiciones para que la medida este bien empleada: El instrumento tiene que tener una sólida base teórica y debe ser de múltiples ítems por razones de fiabilidad (Verplanken & Orbell, 2003).

### Índice de Hábito de Autoinforme (SRHI Self Report Habit Index)

El índice de hábito de auto-informe (SRHI) es una escala de 12 ítems que auto informan el hábito enfocándose en experiencias comunes de automaticidad: eficiencia (Lo hago sin pensarlo), falta de conciencia (Comienzo a hacerlo antes de

que me dé cuenta que lo estoy haciendo) e incontrolabilidad (No hacerlo requerirá esfuerzo), así como también frecuencia de comportamiento (Lo hago frecuentemente) y relevancia para la identidad propia (Es algo típico de mi) (Gardner, 2015).

Los ítems 1, 7 y 12 pertenecen a la frecuencia, los ítems 3, 4 y 10 son calificados como falta de conciencia, falta de control y eficiencia mental respectivamente, ítem 2 como automaticidad general, 5 falta de conciencia, 6, 8 y 9 falta de control y el ítem 11 como único de auto identidad (Gardner & Tang, 2013).

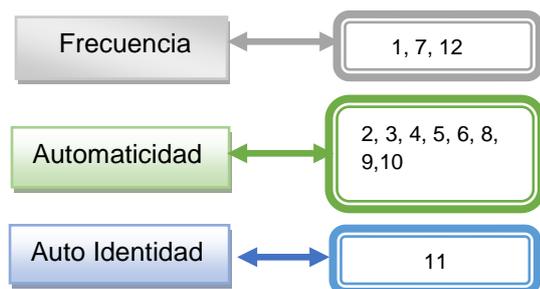


Figura 3: Ítems SRHI  
Elaborado por: Gustavo Vélez y Juan Galán

## METODOLOGÍA

La metodología en este estudio es aplicada en el cuestionario de autoinforme del hábito (SRHI), con un enfoque cualitativo está basado en las experiencias de frecuencia, automaticidad y auto identidad, es una teoría del hábito altamente apropiada para el contexto de este estudio debido a que es un comportamiento social aprendido mediante la observación y costumbres de los funcionarios en el uso de los sistemas de información en el sector hospitalario. El análisis de los datos obtenidos fue procesado mediante el programa estadístico SPSS.

## Participantes

Los participantes para el análisis lo conformaron un promedio de 70 doctores con diferentes especialidades en las áreas de dermatología, pediatría, ginecología, odontología, neumología, cardiología y nefrología con una rango de edad desde 23 a 63 años, 33 hombres y 37 mujeres.

## Instrumento

Para la recopilación de los datos e identificación del comportamiento actual de los funcionarios se utilizaron los 12 ítems del SRHI en relación con 3 escenarios adaptados de las primeras 3 políticas de seguridad de los sistemas de información más relevantes en el Hospital dentro de una escala entre 1 y 5, 1 correspondiente a nunca, 2 casi nunca, 3 a veces, 4 casi siempre y 5 considerado como siempre.

## Procedimiento

Se procedió con el levantamiento de información mediante previa solicitud con el Gerente General del Hospital especificando que la recopilación de información es de propósito académico e investigativo con absoluta confidencialidad y reserva. Con la solicitud aprobada se procedió con la entrevista al Jefe de departamento de TI para identificar las políticas de seguridad de los sistemas de información, el Hospital cuenta con 180 políticas, se estableció la prioridad para analizar las primeras 3 políticas que más infringen o son más vulneradas por los funcionarios. Con base a las 3 políticas de seguridad de los sistemas de información más relevantes para el Hospital se desarrolló un escenario asociado con cada política, incluidos los 12 ítems del SRHI por cada escenario.

Las 70 encuestas fueron entregadas de manera personal a los funcionarios médicos de diferentes especialidades de forma aleatoria.

## ANÁLISIS DE RESULTADOS

Los resultados son mostrados por cada escenario. Se establecieron correlaciones de cada uno de los ítems del SRHI que pertenecen a cada constructo o experiencia común. Se estima una probabilidad mayor o igual a 0.50 en el que confirma si los ítems son idóneos para la medición del hábito (Gutierrez & Pino, 2011).

### Escenario 1

En la tabla 1 se muestra la correlación entre los ítems correspondientes a la frecuencia, las correlaciones representan valores entre 0.61 (P1,P2) a 0.729 (P7,P12).

Inter-Item Correlation Matrix

	P1	P7	P12
P1	1,00	,694	,614
P7	,694	1,00	,729
P12	,614	,729	1,00

Tabla 1: Frecuencia Escenario1  
Fuente SPSS

En la tabla 2, los ítems de automaticidad muestran valores mayores a 0.521 con una excepción en (P4,P9)=0.496

**Inter-Item Correlation Matrix**

	P2	P3	P4	P5	P6	P8	P9	P10
P2	1,00	,882	,534	,895	,603	,741	,707	,733
P3	,882	1,00	,543	,921	,723	,732	,711	,751
P4	,534	,543	1,00	,539	,642	,627	,496	,521
P5	,895	,921	,539	1,00	,659	,763	,740	,760
P6	,603	,723	,642	,659	1,00	,720	,712	,631
P8	,741	,732	,627	,763	,720	1,00	,602	,621
P9	,707	,711	,496	,740	,712	,602	1,00	,698
P10	,733	,751	,521	,760	,631	,621	,698	1,00

Tabla 2 Automaticidad Escenario1  
Fuente SPSS

**Escenario 2**

Los ítems muestran valores mayores o iguales a 0.753 correlacionados con la frecuencia.

**Inter-Item Correlation Matrix**

	P1	P7	P12
P1	1,00	,873	,753
P7	,873	1,00	,776
P12	,753	,776	1,00

Tabla 3 Frecuencia Escenario2  
Fuente SPSS

Referente a los ítems relacionados con la automaticidad, las correlaciones entre (P4,P2), (P4,P3), (P4,P5), (P4,P8), (P4,P9), (P4,P10), (P6,P10), son menores a 0,50 consideradas como menos significativas, representado en la tabla 4.

**Inter-Item Correlation Matrix**

	P2	P3	P4	P5	P6	P8	P9	P10
P2	1,00	,845	,496	,859	,669	,871	,786	,586
P3	,845	1,00	,450	,873	,724	,862	,782	,522
P4	,496	,450	1,00	,452	,542	,427	,305	,458
P5	,859	,873	,452	1,00	,625	,874	,758	,598
P6	,669	,724	,542	,625	1,00	,704	,713	,434
P8	,871	,862	,427	,874	,704	1,00	,874	,643
P9	,786	,782	,305	,758	,713	,874	1,00	,727
P10	,586	,522	,458	,598	,434	,643	,727	1,00

Tabla 4 Automaticidad Escenario2  
Fuente SPSS

**Escenario 3**

Ítems asociados con la frecuencia con valores desde 0.694 en las correlaciones.

**Inter-Item Correlation Matrix**

	P1	P3	P7
P1	1,00	,694	,724
P3	,694	1,00	,925
P7	,724	,925	1,00

Tabla 5 Frecuencia Escenario3  
Fuente SPSS

Para la relación con la automaticidad todas las correlaciones mostraron un valor mayor 0.50 en comparación con los escenarios anteriores.

**Inter-Item Correlation Matrix**

	P2	P3	P4	P5	P6	P8	P9	P10
P2	1,00	,795	,694	,835	,686	,759	,771	,698
P3	,795	1,00	,692	,879	,729	,874	,836	,785
P4	,694	,692	1,00	,658	,616	,710	,713	,556
P5	,835	,879	,658	1,00	,695	,868	,835	,812
P6	,686	,729	,616	,695	1,00	,788	,826	,660
P8	,759	,874	,710	,868	,788	1,00	,931	,867
P9	,771	,836	,713	,835	,826	,931	1,00	,832
P10	,698	,785	,556	,812	,660	,867	,832	1,00

Tabla 6 Automaticidad Escenario3  
Fuente SPSS

**Análisis General**

En base a los resultados de los 3 escenarios los ítems asociados con la frecuencia mostraron valores mayores a 0.65 en todas sus correlaciones mientras que con los ítems de automaticidad la correlación con el ítem 4 y 9 (P4) y (P9) en el escenario 1 resultó de una mínima posibilidad de ser igual a 0.50 y en el escenario 2 la correlación del ítem 4 fue menor a 0.50 incluyendo la correlación del ítem 6 y 10 (P6, P10), los ítems restantes en todas sus correlacion es resultaron de un valor mayor a 0.50.

Los 12 ítems han sido altamente consistentes, se logró identificar su validez y fiabilidad sin embargo se establece que cuando existen ítems fuertemente intercorrelacionados (como en este caso los ítems de automaticidad) son altamente redundantes. Cuando se incluye un ítem a una escala de medición, el otro contribuye con información poco significativa, la respuesta de los ítems juntos debería de ser similar, pero así también juntos proporcionarían información menos incremental que al incluir un sólo ítem. (Clark & Watson, 1995)

**CONCLUSIONES, LIMITACIONES Y TRABAJOS FUTUROS**

Se cumplió con el objetivo de evaluar el cuestionario de auto informe SRHI analizando la correlación de cada uno de los ítems con escenarios que se adaptan con las primeras 3 políticas de seguridad de los sistemas de información más relevantes en el Hospital.

El SRHI ha demostrado ser una escala muy fiable para la medición del hábito, sin embargo sería importante revisar con el Gerente de TI en mayor detalle el ítem 4 asociado con la política de seguridad de los sistemas de información así como también ampliar la muestra para identificar en futuros estudios la existencia de ítems redundantes e identificar su validez y fiabilidad.

Considerado como una limitante, el tamaño de la muestra y la cantidad de empresas, debido a la evaluación en este análisis los resultados del Hospital no se pueden comparar con los resultados de otra empresa similar o diferente, sea esta del sector público o privado.

Un factor importante es la empresa objeto de análisis, el sector hospitalario donde se almacena gran cantidad de información referente a datos personales de cada paciente como su historial clínico, los funcionarios médicos tienen turnos de trabajo donde varios funcionarios comparten sus contraseñas para ingresar a los sistemas de información, evidenciado en el levantamiento de información y en las políticas más relevantes en el Hospital, por tal motivo es recomendable establecer campañas de concientización en el buen uso de credenciales de acceso y protección de la información.

Establecer alternativas en los mecanismos de autenticación que pueda reemplazar el uso de contraseñas por ejemplo la huella dactilar, reconocimiento facial y verificación de patrones oculares como la retina e iris, estos mecanismos son bastante efectivos para confirmar la identidad de forma inequívoca.

El estudio genera una visión global no solamente desde la perspectiva tecnológica, también desde otras disciplinas como la social o psicológica que pueda determinar un enfoque real del problema. El ser humano de manera intencional o no intencional está involucrado en comportamientos que ponen en peligro los recursos de la organización.

**BIBLIOGRAFÍA**

Aarts, H. a. (2000). The Automatic Activation of Goal- Directed Behaviour: The Case of

Travel Habit. *Journal of Environmental Psychology* (20:1), 75-82.

Aarts, H. P. (1997). "Physical Exercise Habit: On the Conceptualization Formation of Habitual Health Behaviours. *Health Education Research* (12:3),, 363-374.

Ajzen, I. (1985). "From Intentions to Actions: A Theory of Planned Behavior," in *Action Control: From Cognition to Behavior*. J. Kuhl, and J. Beckmann (eds.), New York: Springer Verlag, 11-39.

Ajzen, I. (1991). The Theory of Planned Behavior. *ORGANIZATIONAL BEHAVIOR AND HUMAN DECISION PROCESSES* , 179-211.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 179-211.

Ajzen, I. a. (1986). Prediction of Goal Directed Behaviors: Attitudes, Intentions, and Perceived Behavioral Control. *Journal of Experimental Social Psychology*, 453-474.

Anderson, E. W. (1993). The Antecedents and Consequences of Customer Satisfaction for Firms. *Marketing Science* (12:2), , 125-143.

Aytes, K. &. (2003). A research model for investigating human behavior related to computer security. *Proceedings of the 2003 American Conference on Information Systems, Tampa*, 4-6.

Aytes, K. &. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing*, 22-40.

Barki, J. L. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly*, 503-522.

Bhattacharjee, A. (2001). An Empirical Analysis of the Antecedents of Electronic Commerce Service Continuance. *Decision Support Systems* (32:2), 201-214.

Bulgurcu, B. C. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information

- security awareness. *MIS Quarterly*, 523–548.
- Cao, L. (2004). Major criminological theories: Concepts and measurement. Belmont. CA: Wadsworth.
- Carte, T. A. (2003). In Pursuit of Moderation: Nine Common Errors and Their Solutions. *MIS Quarterly* (27:3), 479-501.
- Chan, M. W. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, 18-41.
- Charng, H.-W. P. (1988). Role Identity and Reasoned Action in the Prediction of Repeated Behavior. *Social Psychology Quarterly* (51:4), 303-317.
- Clark, L. A., & Watson, D. (1995). Constructing Validity: Basic Issues in Objective Scale Development. *American Psychological Association*, 309-319.
- Dabolkar, P. A., Shepard, C. D., & and Thorpe, D. I. (2000). A Comprehensive Framework for Service Quality: An Investigation of Critical Conceptual and Measurement Issues Through a Longitudinal Study. *Journal of Retailing* (76:2), 139-173.
- D'Arcy, J. H. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 79–98.
- Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 318-339.
- Davis, F. D. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, 982-1003.
- Egelman, S. (2015). Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). *Proc. ACM CHI'15 Conf. Hum. Factors Comput. Syst*, 2873-2882.
- Fazio, R. (1990). Multiple processes by which attitudes guide behavior: The mode. *Advances in Experimental Social Psychology*, 75-109.
- Fishbein, M. a. (1975). Attitude, Intention and Behavior: An Introduction to Theory and Research, Reading. MA: Addison-Wesley Publishing Company.
- Gardner, B. (2015). A review and analysis of the use of 'habit' in understanding, predicting and influencing health related behaviour. *Health Psychology Review*, 277-295.
- Gardner, B., & Tang, V. (2013). Reflecting on non-reflective action: An exploratory think-aloud study of self-report habit measures. *British Journal of Health Psychology*, 258-273.
- Gardner, B., Abraham, C., Lally, P., & de Bruijn, G.-J. (2012). Towards parsimony in habit measurement: Testing the convergent and predictive validity of an automaticity subscale of the Self-Report Habit. *International Journal of Behavioral Nutrition and Physical Activity*, 1-12.
- Gardner, B., Abraham, C., Phillippa, L., & de Bruijn, G.-J. (2011). The Habitual Use of the Self-report Habit Index: A Reply. *Annals of Behavioural Medicine*, 141-142.
- Goeken, D. M. (2013). Social factors in policy compliance - Evidence found in literature to assist the development of policies in information security management. *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 4476-4484.
- Guo, K. H. (2013). Revisiting the Human Factor in Organizational Information Security Management. *ISACA J*, 1-5.
- Gutierrez, S. A., & Pino, J. M. (2011). Validacion de la version en español de las propiedades psicosometricas de la escala SRHI para medir habitos de ejercicio fisico. *Rev Esp Salud Pública*, 363-371.
- Hagen, J. (2009). Human relationships: A never-ending security education challenge. *Security & Privacy*, 65-67.
- Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse

- judgments and intentions. *MIS Quarterly*, 257–278.
- Hartwick, J. a. (1994). “Explaining the Role of User Participation in Information Systems Use,”. *Management Science* (40:4), 440-465.
- Herath, J. D. (2011). A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings. *Eur. J. Inf. Syst.*, vol. 20, no. 6, 643-658.
- Herath, T. &. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47, 54–165.
- J. M. Stanton, K. R. (2005). “Analysis of end user security behaviors,”. *Comput. Secur.*, vol. 24, no. 2, 124-133.
- Jai-Yeol, S. (2011). Out of fear or desire? Toward a better understanding of employees’ motivation to follow IS security policies *Information and Management* . 296–302.
- K. Bagchi, G. U. (2003). , An analysis of the growth of computer and internet security breaches. *Communications of the Association for Information Systems*, 684–700.
- Karahanna, E. S. (1999). Information Technology Adoption Across Time: a Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs. *MIS Quarterly* (23:2), 183-213.
- Kim, S. M. (2005). Two competing perspectives on automatic use: a theoretical and empirical comparison. *Information Systems Research*, 418-432.
- L. Myyry, M. S. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study . *European Journal of Information Systems*, 126–139.
- Lally, P., & Gardner, B. (2013). Promoting habit formation. *Health Psychology Review*, 137-158.
- Lee, S. M.-G. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management* 41(6), 707-718.
- Leidner, P. B. (2017). Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory. *ACM SIGMIS Database DATABASE Adv. Inf. Syst.*, vol. 48,, 11-43.
- Limayem, M. H. (2007). How habit limits the predictive power of intentions: the case of IS continuance. *MIS Quarterly* (31:4), 705-737.
- M. Alaskar, S. V. (4241-4250). Evolvement of Information Security Research on Employees’ Behavior: A Systematic Review and Future Direction. *Hawaii International Conference on System Sciences*, 2015.
- M. Limayem, S. H. (2003). Force of habit and information systems usage: theory and initial validation. *Journal of the AIS*, 65–97.
- M. Siponen, R. W. (2009). Information security management standards: problems and solutions. *Information and Management* , 267–270.
- M. Siponen, S. P. (2010). Compliance with information security policies: An empirical investigation. *Computer (Long. Beach. Calif)*, 64-71.
- Mathieson, K. (1991). “Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior,”. *Information Systems Research* (2:3), 173-191.
- Moore, G. C. (1991). Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. *Information Systems Research* (2:3), 192-222.
- Moore, G. C. (1996). Integrating Diffusion of Innovations and Theory of Reasoned Action Models to Predict Utilization of Information Technology by End-Users. *in Diffusion and Adoption of Information*

- Technology, K. Kautz and J. Pries-Heje  
.London: Chapman & Hall, 132-146.
- Myyry, L. S. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, 126-139.
- Neal, D., & Wood, W. (2007). A New Look at Habits and the Habit–Goal Interface. *Physiological Review*, 843-863.
- Neal, D., Vujcic, J., Hernandez, O., & Wood, W. (2015). The science of habit creating disruptive and sticky behavior change in handwashing behavior. *Washplus*, 24.
- Neal, D., Wood, W., & Quinn, J. (2006). Habits A Repeat Performance. *Current Directions in Psychological Science*, 198-202.
- Neal, D., Wood, W., Wu, M., & Kurlander, D. (2011). The Pull of the Past: When Do Habits Persist Despite Conflict With Motives? *Personality and Social Psychology*, 1428-1437.
- Ng, B. K. (2009). Studying users' computer security behavior using the health belief model. *Decision Support Systems*, 815–825.
- Oullette, J., & Wood, W. (1998). Habit and Intention in Everyday Life: The Multiple Processes by Which Past Behavior. *Psychological Bulletin*, 54-74.
- P. Puhakainen, M. S. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 757–778.
- Pahnila, S. S. (2007). Which factors explain employees' adherence to information security policies? An empirical study, Proceedings of the PACIS . *Auckland, New Zealand*.
- Poldrack, R., Clark, J., Paré-Blagoev, E. J., Shohamy, D., Moyano, J. C., Myers, C. E., & Gluck, M. (2001). Interactive memory systems in the human brain. *Nature*, 6.
- Puhakainen, P. (2006). Design theory for information security awareness. *Unpublished doctoral dissertation*.
- Rogers. (1995). E. M. Diffusion of Innovations (4th ed.). *New York: The Free Press*.
- Rogers, E. M. (1983). Diffusion of Innovations (3rd ed.). *New York: The Free Press*.
- S.M. Lee, S. L. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management*, 707-718.
- Siponen, M. &. (2006). IS security design theory framework and six approaches to the application of IS security policies and guidelines. *Journal of the Association for Information Systems*, , 445–472.
- Siponen, M. &. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. . *MIS Quarterly*, , 487–502.
- Siponen, M. M. (2010). Why employees don't comply with information security policies: An empirical investigation. . *IEEE Computer*, 64–71.
- Siponen, M. T. (2000). A conceptual foundation for organizational IS security awareness. *Information Management & Computer Security*, 31–41.
- Stanton, J. S. (2005). Analysis of end user security behaviors. *Computers and Security*, 124–133.
- Straub, D. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, 255–276.
- Taylor, S. a. (1995). Assessing IT Usage: The Role of Prior Experience. *MIS Quarterly (19:4)*, 561-570.
- Thorngate, W. (1976). Must We Always Think Before We Act? *Personality of Social Psychology Bulletin (2:1)*, 31-35.
- Verplanken, B. a. (2003). Reflections on Past Behavior: A Self-Report Index of Habit Strength. *Journal of Applied Social Psychology (33:6)*, 1313-1330.

- Verplanken, B., & Aarts, H. (1999). Habit, Attitude, and Planned Behaviour: Is Habit an Empty Construct or an Interesting Case of Goal-directed. *European Review of Social Psychology*, 101-134.
- Verplanken, B., & Orbell, S. (2003). Reflections on Past Behavior A Self-Report Index of Habit Strength. *Journal of Applied Social Psychology*, 1313-1330.
- Verplanken, B., & Orbell, S. (2010). The Automatic Component of Habit in Health Behavior: Habit as Cue-Contingent Automaticity. *Health Psychology*, 374-383.
- Verplanken, B., & Sheina, O. (2015). The strenght of habit. *Health Psychology Review*, 10.
- Warshaw, P. R. (1984). Self-Understanding and the Accuracy of Behavioral Expectations. *Personality and Social Psychology Bulletin* (10:1), 111-118.
- Warshaw, P. R. (1985a). The Accuracy of Behavioral Intention Versus Behavioral Expectation for Predicting Behavioral Goals. *Journal of Psychology* (119:6), 599-602.
- Warshaw, P. R. (1985b). Disentangling Behavioral Intention and Behavioral Expectation. *Journal of Experimental Social Psychology* (21:3), 213-228.
- Wittenbraker, J. G. (1983). Seat Belt Attitudes, Habits, and Behaviors: An Adaptive Amendment to the Fishbein Model. *Journal of Applied Social Psychology* (13:5), 406-421.
- Wood, W. (2017). Habit in Personality and Social Psychology. *Personality and Social Psychology Review*, 1-15.
- Wood, W., & Runger, D. (2016). Psychology of Habit. *Annual Review of Psychology*, 27.
- Wood, W., Jeffrey, Q., & Kashy, D. (2002). Habits in Everyday Life: Thought, Emotion, and Action. *Personality and Social Psychology*, 1281-1297.
- Young, E. &. (2008). *global information security survey*.

**Anexo 1: Encuesta Escenarios**

Edad		Genero	H	
			M	
Especialista en:				
Religión	Católica			
	Testigo de Jehová			
	Evangelista			
	Otra			

**ENCUESTA**

Estimado/a profesional, la siguiente encuesta está realizada con la finalidad de obtener datos sobre su comportamiento rutinario en cuanto a su seguridad tecnológica que lleva dentro de su trabajo, y que ayudará a desarrollar la tesis de estudio de sistemas de seguridad en el H. V. C. Moscoso. Por lo que se agradece su sinceridad al momento de responder, así como la seguridad de que los datos serán utilizados solo para dicha investigación.

**ESCENARIO 1**

Julia tiene acceso a información de la empresa en la que labora, mediante la utilización de un servidor de archivos al cual ingresa mediante su contraseña personal. Julia tuvo que salir urgente de la ciudad y recibe una llamada de su compañero Fabián quien necesita de urgencia un archivo de este servidor, por lo que Julia comparte su contraseña con su compañero de trabajo.

En base a este escenario, señale con una **X**, como sería su comportamiento en situaciones comparables con las de Julia en una escala de 1 a 5; siendo:

**1 = nunca    2 = casi nunca    3 = a veces    4 = casi siempre    5 = siempre**

Código	El comportamiento de Julia es algo que	1	2	3	4	5
1	Lo hace frecuentemente					
2	Lo hace automáticamente					
3	Lo hace sin tener conscientemente que recordarlo					
4	Se siento raro/a o extraño/a si no lo hace					
5	Lo hace sin necesidad de pensarlo					
6	No hacerlo requeriría de esfuerzo					
7	Es parte de su rutina (diaria, semanal, mensual)					
8	Comienza a hacerlo antes de que me se cuenta que lo esta haciendo					
9	Encontraría difícil no hacerlo					
10	No ha necesitado pensar sobre ello para hacerlo					
11	Es algo típico de usted					
12	Ha estado haciéndolo durante largo tiempo					

**ESCENARIO 2**

Karla tiene licencia por calamidad doméstica y sale dos horas antes de su jornada laboral, ella no ha podido terminar una tarea urgente, le pide a su compañera/ro y mejor amiga/o, quien está ubicada dos cubículos hacia la derecha de ella, que por favor le ayude finalizando esta tarea, la compañera/ro acepta en ayudarla. Karla deja en su escritorio su contraseña escrita en un papel antes de irse.

En base a este escenario, señale con una **X**, como sería su comportamiento en situaciones comparables con las de Karla en una escala de 1 a 5; siendo:

**1** = nunca    **2** = casi nunca    **3** = a veces    **4** = casi siempre    **5** = siempre

Código	El comportamiento de Julia es algo que	1	2	3	4	5
1	Lo hace frecuentemente					
2	Lo hace automáticamente					
3	Lo hace sin tener conscientemente que recordarlo					
4	Se siento raro/a o extraño/a si no lo hace					
5	Lo hace sin necesidad de pensarlo					
6	No hacerlo requeriría de esfuerzo					
7	Es parte de su rutina (diaria, semanal, mensual)					
8	Comienza a hacerlo antes de que me se cuenta que lo esta haciendo					
9	Encontraría difícil no hacerlo					
10	No ha necesitado pensar sobre ello para hacerlo					
11	Es algo típico de usted					
12	Ha estado haciéndolo durante largo tiempo					

**ESCENARIO 3**

Juan ingresa su contraseña de usuario desde su computador para iniciar su turno de trabajo, en la pantalla le muestra un mensaje de que su contraseña expira en 5 días desea cambiarla ahora si/no, Juan aprovecha en cambiar su contraseña. Juan prefiere utilizar una contraseña que se le haga fácil de digitar y recordar cada vez que inicie sesión como por ejemplo el nombre de su esposa.

En base a este escenario, señale con una **X**, como sería su comportamiento en situaciones comparables con las de Juan en una escala de 1 a 5; siendo:

**1** = nunca    **2** = casi nunca    **3** = a veces    **4** = casi siempre    **5** = siempre

Código	El comportamiento de Juan es algo que	1	2	3	4	5
1	Lo hace frecuentemente					
2	Lo hace automáticamente					
3	Lo hace sin tener conscientemente que recordarlo					
4	Se siento raro/a o extraño/a si no lo hace					
5	Lo hace sin necesidad de pensarlo					
6	No hacerlo requeriría de esfuerzo					
7	Es parte de su rutina (diaria, semanal, mensual)					
8	Comienza a hacerlo antes de que me se cuenta que lo esta haciendo					
9	Encontraría difícil no hacerlo					
10	No ha necesitado pensar sobre ello para hacerlo					
11	Es algo típico de usted					
12	Ha estado haciéndolo durante largo tiempo					