JORNADA DE INVESTIGACIÓN 2024. FACULTAD CIENCIAS ECONÓMICAS Y EMPRESARIALES - USAL, Buenos Aires, 2024.

Modelo capacitación y sensibilización en ciberseguridad para Contadores Públicos.

Diego Sebastián Escobar.

Cita:

Diego Sebastián Escobar (2024). *Modelo capacitación y sensibilización en ciberseguridad para Contadores Públicos. JORNADA DE INVESTIGACIÓN 2024. FACULTAD CIENCIAS ECONÓMICAS Y EMPRESARIALES - USAL, Buenos Aires.*

Dirección estable: https://www.aacademica.org/escobards/77

ARK: https://n2t.net/ark:/13683/ptuD/70g

UNIVERSIDAD DEL SALVADOR

FACULTAD CIENCIAS ECONÓMICAS Y EMPRESARIALES

JORNADA DE INVESTIGACIÓN

Martes 17 de septiembre de 2024

Título: “Modelo capacitación y sensibilización en ciberseguridad para Contadores Públicos”

Autor: Diego Sebastián Escobar

Profesor Adjunto de Tecnología de la información. Facultad de Ciencias Económicas y Empresariales. USAL.

Índice temático

1. Introducción

En el marco de la Segunda Jornada Institucional de Investigación de la Universidad del Salvador, presentamos el trabajo titulado “Modelo de Capacitación y Sensibilización en Ciberseguridad para Contadores Públicos”.

El objetivo principal de este estudio es proponer un modelo simplificado para la gestión de la capacitación en ciberseguridad, específicamente diseñado para profesionales en Ciencias Económicas, con énfasis en Contadores Públicos.

Al desarrollar un programa de concientización y capacitación en ciberseguridad para Contadores Públicos, es crucial considerar varios aspectos. Este artículo analiza las herramientas que permiten diagnosticar las conductas de los usuarios y de los atacantes en una organización, estableciendo las bases teóricas para un modelo tripartito de concientización en seguridad.

En la primera sección, se identifican las recomendaciones consideradas para el desarrollo del modelo propuesto, dirigido a este tipo de entidades. En la segunda sección, se presenta una síntesis de la propuesta desarrollada, enfocada específicamente en las entidades objeto de estudio.

2. Planes de concientización: características a ser consideradas.

Los autores Tipton H. y Krause M. en su libro: (Information Security Management Handbook, 2005)i fundamentan que “las actitudes se definen como nuestra respuesta positiva o negativa a algo.” Asimismo, afirman que los profesionales en seguridad tienen que ser conscientes de las actitudes de los usuarios finales por las siguientes tres razones:

a. Conductas de las personas en un programa de concientización

Para predecir el comportamiento

- *"Las actitudes son un buen predictor de la conducta. Es por eso que las encuestas son una herramienta muy valiosa en un programa de seguridad en general. Si puede determinar las actitudes de la población objetivo hacia los problemas de seguridad de información, tales como la privacidad y la confidencialidad , puede utilizar esa información para predecir qué tan seguro será su medio ambiente."*

Los objetivos del cambio

- *"Las actitudes pueden ser objeto de cambio. Si sutil o directamente puede cambiar la actitud de alguien, puede cambiar el comportamiento en consecuencia . A menudo es más fácil cambiar el comportamiento a través de un cambio de actitud que cambiar el comportamiento directamente."*

Fuente del riesgo

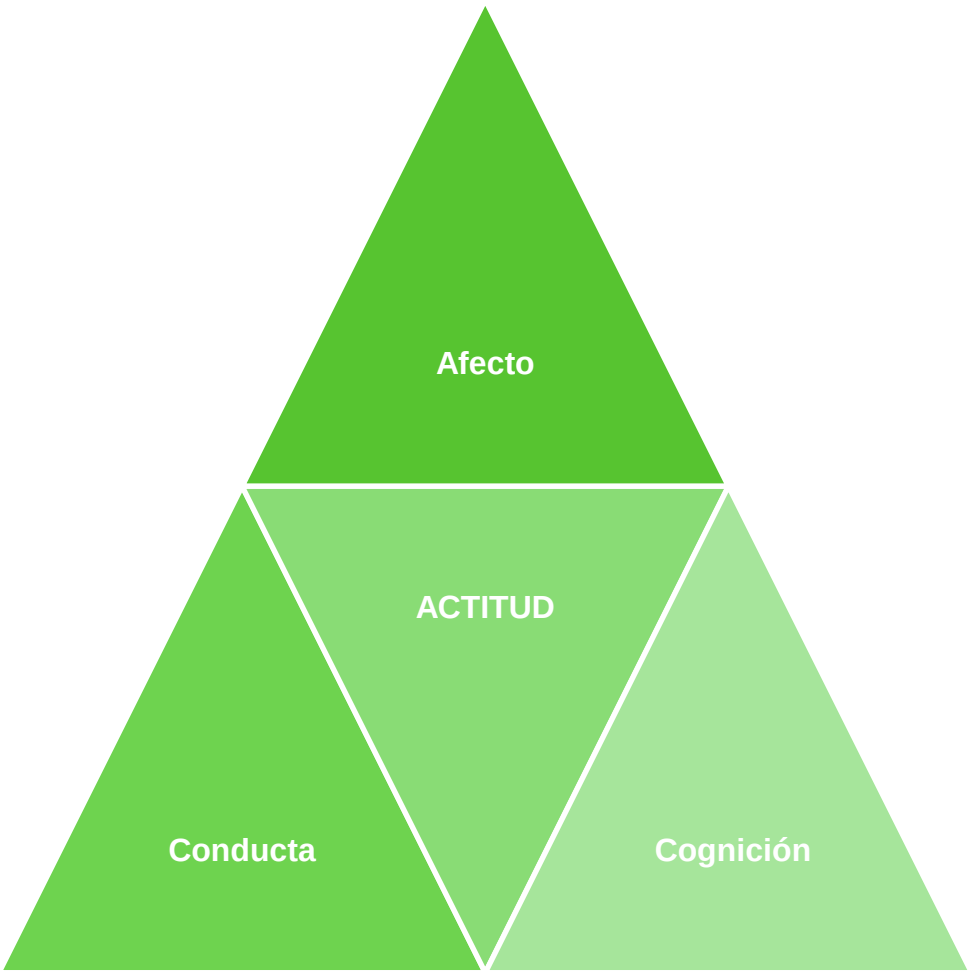
- *"Las actitudes son una fuente de riesgo para un profesional de la seguridad de la información. Actitudes extremas hacia alguien o algo puede conducir a la función cognitiva y el comportamiento irracional. Esta es una de las situaciones más temidas por un administrador de seguridad de la información, ya que no se puede predecir racionalmente. "*

Fuente: Basado en (Tipton & Krause, Information Security Management Handbook, 2005)

El modelo Tripartito del individuo en la Concientización de la Seguridad (Tipton & Krause, Attitude Structure and Function: The ABC's of the Tripartite Model, 2005)ii

Al identificar a los destinatarios del programa de capacitación, El modelo tripartito (también conocido como el modelo ABC) presenta la actitud como una amalgama de tres componentes: afecto, conducta y cognición.

b. El Modelo Tripartito de Concientización de la Seguridad



Fuente: Basado en (Tipton & Krause, Attitude Structure and Function: The ABC's of the Tripartite Model, 2005)

c. Análisis preliminar del modelo

En la siguiente tabla se analizan brevemente cada una de las partes pertinentes del modelo:

Modelo Tripartito para analizar al individuo

Modelo		
1	Afecto	*"El componente afectivo es el aspecto emocional de nuestras actitudes. Nuestros sentimientos hacia un objeto o sujeto juegan un papel importante en la determinación de*

		nuestras actitudes."[iii]
2	Comportamiento	*"El componente de comportamiento se deriva del hecho de que nuestro comportamiento sirve como un mecanismo de retroalimentación para nuestras actitudes. En definitiva, "hacer" conduce a "me gusta"*[iv]*.*
3	Cognición	*"El componente cognitivo es la reflexiva, pensando aspecto de nuestras actitudes".*[v]

Fuente: (Tipton & Krause, Attitude Structure and Function: The ABC's of the Tripartite Model, 2005)

Teniendo en cuenta el "afecto" que tienen las personas, el "programa de concienciación sobre la seguridad" puede desarrollarse teniendo en cuenta las respuestas emocionales. Se pueden dar ejemplos, videos o casos de phishing, robo de claves en cajeros automáticos o robo de identidad.

Analizando el comportamiento, se podría enseñar y ejemplificar con el uso de experimentos. Como por ejemplo, cómo se guardan las contraseñas en un Sistema Operativo, cómo los delincuentes utilizan técnicas de skimming para robar datos de tarjetas de créditos, o reunirlos en grupo para que analicen perfiles en las redes sociales o cómo se incumple con la ley de protección de datos personales en la Argentina.

Y por último, contemplando la Cognición, se los podría hacer reflexionar sobre el manejo y cuidado de la información, en el caso de existir un robo de equipos ya sean notebooks, tabletas o celulares, o ejemplos acerca de cómo se pueden filtrar diferentes videos en la web y causar perjuicios.

3. Estándares y buenas prácticas analizadas para gestionar la Seguridad de la Información de sistemas contables.

El Sistema de Gestión de Seguridad de la Información es definido como un "Proceso sistemático, documentado y conocido por toda la organización. Y basado en un enfoque por riesgo de negocio, el SGSI es un modelo para el establecimiento, implementación, operación, control, revisión, mantenimiento y mejora de la seguridad de la información." (ISO/IEC/IRAM 27.001).
La misma establece los siguientes 11 dominios mínimos a tener en cuenta para implantar en la Gestión de la Seguridad:

Cuadro N°1: Dominios de la ISO/IEC/IRAM 27.001	
Aspectos cubiertos por la norma ISO/IEC 27.001	1. Política de Seguridad.
	2. Organización de Seguridad de la Información.
	3. Administración de Activos.
	4. Gestión de Recursos Humanos.
	5. Seguridad Física y Ambiental.
	Gestión de operaciones y comunicaciones.
	7. Control de Acceso.
	8. Adquisición, Desarrollo y Mantenimiento de sistemas.
	9. Gestión de incidentes.
	10. Administración de la Continuidad de los Negocios.
	11. Cumplimiento de la normativa Legal Vigente.
Fuente: ISO/IEC 27.001	

El autor subraya que cada uno de los aspectos abordados corresponde a características de los sistemas de gestión de la seguridad que no están exclusivamente relacionados con términos tecnológicos. En la administración de la seguridad, es necesario redactar políticas estratégicas, normas, procedimientos, inventarios de activos de información y establecer controles sobre los procesos en las entidades.

Considerando estos dominios, se pueden relacionar con las diferentes decisiones y funciones tomadas en los niveles de la organización, las cuales se subdividen en decisiones estratégicas, tácticas y operativas.

Cuadro N° 2: Niveles organizacionales y los dominios establecidos por la ISO/IEC/IRAM 27.001.

Fuente: Análisis propio a partir de la ISO/IEC/IRAM 27.001

4. Reflexiones a modo de conclusiones

a. Medidas estratégicas

Dentro de las medidas estratégicas, las organizaciones tienen que establecer una política de seguridad de la información para todos los integrantes y establecer los roles para la organización de la seguridad; dadas las características de los micro y pequeños entes no se necesitan estructuras burocráticas, pero si establecer roles y funciones internos.

1. Política de Seguridad
Las organizaciones tienen que establecer un documento de alto nivel en donde se defina la política de seguridad de la información y una revisión anual de la misma.

2. Organización de la seguridad de la información
En lo que respecta a la organización interna, se tiene que enfatizar en el compromiso de los máximos responsables en los entes sobre la seguridad de la información y se deberían asignar las responsabilidades en roles y funciones en la misma.

b. Medidas tácticas

En relación con las medidas tácticas a implementar, se deben establecer procedimientos para la gestión de recursos humanos, cumplimiento de la ley de protección de datos personales y administración de la continuidad del negocio.

3 . Gestión de las comunicaciones y operaciones
Los entes deben implementar una correcta gestión de las comunicaciones y operaciones en relación a la las copias de respaldo o Backup.

4. Gestión de recursos humanos
Establecer las medidas necesarias antes del empleo, incluyendo capacitación y concientización sobre medidas sobre ciberseguridad, firmar los convenios de confidencialidad necesarios y una vez terminada la relación contractual que se devuelva la información contenida en equipos y en formato de papel.

5. Cumplimiento legal
Los entes deben cumplir con lo dispuesto en la Ley de proyección de datos personales y las disposiciones de la Agencia de Accesos a la Información Pública en el ámbito de la República Argentina.

6. Administración de la continuidad del negocio
Las organizaciones deben gestionar los riesgos y la continuidad del negocio, como también administrar el mantenimiento y evaluación de los planes de continuidad del negocio en caso de diferentes escenarios en donde peligre la continuidad operativa.

c. Medidas operativas

En relación con las medidas operativas, las micro y pymes de servicios, deben establecer medidas sobre el control de acceso lógico y físico, poseer un plan operativo anual sobre la adquisición de tecnología, gestión de incidentes y gestión de los activos de información.

7. Control del acceso
Los entes tienen que establecer los requerimientos de los controles lógicos a los sistemas operativos, aplicativos y servicios por internet. Todos los accesos deben tener una política de contraseñas y configurar segundo factor de autenticación.

8. Seguridad física y ambiental
Los entes tienen que establecer áreas físicamente seguras, para el resguardo de equipos e información sensible.

9. Adquisición, desarrollo y mantenimiento de los sistemas de información
Los entes deben establecer un plan anual para la inversión en equipos y herramientas de seguridad.

10. Gestión de un incidente en la seguridad de la información
Los deben establecer un control y monitoreo de los incidentes que afecten la disponibilidad, confidencialidad e integridad de las operaciones.

11. Administración de activos
Los entes necesitan tener un inventario de activos de información para identificar toda la información que tienen, establecer las responsabilidades, lineamientos de clasificación, etiquetado y manejo de la información corporativa.

Por todo lo expuesto, los profesionales deberían considerar la aplicación de las medidas estratégicas, tácticas y operativas mencionadas para administrar eficientemente la Seguridad de la Información y estar preparados para posibles incidentes que puedan afectar sus operaciones.

Asimismo, se destaca que en la gestión de la ciberseguridad, solo un 20% corresponde a la implementación de herramientas o software específico, mientras que el 80% restante se refiere a tareas de gestión y control. Esto requiere un abordaje interdisciplinario de la seguridad, que abarque desde el análisis crítico de los riesgos existentes hasta una revisión de las necesidades del negocio en cada entidad.

5. Bibliografía

Escobar, D. S. (2010), “Aportes de la Ley de Protección de datos personales en el Sistema de Información Contable. Nuevos conocimientos del Contador Público en la era de la información.” 18º Congreso Nacional de Profesionales en Ciencias Económicas”, Ciudad Autónoma de Buenos Aires.

Escobar, D. S. (2022). Capacitación y concientización en seguridad de la información. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (2-2), 1-6.

Escobar, D. S. (2023). Asegurando la Resiliencia Empresarial: Conceptos fundamentales a considerar en la auditoría de la continuidad del negocio. XXXV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. CGCE, Buenos Aires.

Escobar, D. S. (2023). Asegurando la Resiliencia Empresarial: Conceptos fundamentales a considerar en la auditoría de la continuidad del negocio. XXXV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. CGCE, Buenos Aires.

Escobar, D. S. (2023). Características a considerar en la elaboración de planes de concientización en Ciberseguridad para Contadores Públicos. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (3-1), 1-7.

Diego Sebastián Escobar (2023). CIBERRESILIENCIA: UN NUEVO DESAFÍO EN LA FORMACIÓN DEL CONTADOR PÚBLICO. XLIV Simposio Nacional de Profesores de Práctica Profesional. Universidad Nacional de Córdoba, Cordoba.

Escobar, D. S. (2023). EL IMPACTO DE LAS NUEVAS TECNOLOGÍAS DE INFORMACIÓN EN LA FORMACIÓN PROFESIONAL DEL CONTADOR. XLIV Simposio Nacional de Profesores de Práctica Profesional. Universidad Nacional de Córdoba, Cordoba.

Escobar, D. S. (2010), “Ley de Protección de Datos Personales, Revista Imagen Profesional”, de La Federación Argentina de Consejos Profesionales en Ciencias Económicas. Buenos Aires.

Escobar, D. S. (2014), “El Sistema de Gestión de Seguridad de la Información y las incumbencias profesionales del Contador Público.” Área: Actualización de contenidos programáticos. XXXV Simposio Nacional de Profesores de Práctica Profesional. Concordia.

Escobar, D. S. (2014), “Gestión de mejoras prácticas y estándares de control y tecnologías en los sistemas contables”, Asociación Interamericana de Contabilidad”, Octubre 2014.Comisión Técnica de Sistemas y Tecnologías de Información, Charla Cibernética.

Escobar, D. S. (2014), “Implicancias legales de la Firma Digital y Electrónica en el resguardo de documentación respaldatoria y registros contables.” Presentado en la VII JORNADA NACIONAL DE DERECHO CONTABLE, Junio de 2014, Consejo Profesional de Ciencias Económicas de Santa Fe, Ciudad de Rosario.

Escobar, D. S. (2022). El rol del Contador en la era digital. In VI Jornadas de Orientación Vocacional. UBA.

Escobar, D. S. (2023). Asegurando la Resiliencia Empresarial: Conceptos fundamentales a considerar en la auditoría de la continuidad del negocio. In XXXV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. CGCE.

Escobar, D. S. y otros. “Aspectos legales y formales del sistema de registro “Legal Forma”, Comisión de Estudios sobre Sistemas de Registros, su integridad y autenticidad documental, Informe 1, EDICION, Buenos Aires.

Escobar, Diego Sebastián. (2013). Seguridad informática en los sistemas contables : Un análisis de los aspectos legales, normativos y tecnológicos de la seguridad de la información en el almacenamiento, procesamiento, control y resguardo de los registros contables. (Trabajo Final de Posgrado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0817_EscobarDS.pdf

International Organization for Standardization - International Electrotechnical Commission. (2013), ISO/IEC 27.001 Information technology - Security techniques - Information security management systems - Requirements. Edición Digital.

IT Governance Institute, (2013), “Objetivos de Control para Información y Tecnologías Relacionadas” (COBIT 5, Control Objectives for Information and related Technology). ISACA (Information Systems Audit and Control Association). Accedido desde www.itgi.org

Laudon, K, y Laudon, J. (2012), "Sistemas de Información Gerencial", Editorial. Prentice Hall, Hispanoamericana, México.

[i] Traducción de Social Science, Psychology, and Security Awareness: Why? Fuente: Tipton H. y Krause M. (2005).

[ii] Traducción de “Attitude Structure and Function: The ABC's of the Tripartite Model”, Tipton H. y Krause M. (2005).

[iii] Traducido de: *1. Affect.* The affective component is the emotional aspect of our attitudes. Our feelings toward an object or subject play an important role in determining our attitudes. We are more likely to participate and do things that make us feel happy or good. Our aversion to things that elicit feelings of guilt, pain, fear, or grief can be used to change attitudes and, eventually, behavior. Fuente: Tipton H. y Krause M. (2005).

[iv] Traducido de: *2. Behavior.* The behavior component is derived from the fact that our behavior serves as a feedback mechanism for our attitudes. In short, "doing" leads to "liking." In an ingenious experiment, two randomly selected groups of subjects were asked to rate how much they liked a cartoon they were watching. The two groups watched the same cartoon, with only one group biting a pencil to

simulate the facial muscles of a smile. It was found that the group that had to bite on a pencil rated the cartoon as being much more amusing and likeable than the group that did not. Fuente: Tipton H. y Krause M. (2005).

[v] Traducido de *3. Cognition.* The cognitive component is the thoughtful, thinking aspect of our attitudes. Opinions toward an object or subject can be developed based solely on insightful, process-based thinking. It is no wonder that the nature of TV commercials during news programs is radically different than that aired on Saturday mornings. During news programs, people are more likely to be processing information and "thinking.” Fuente: Tipton H. y Krause M. (2005).