Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, núm. 2-3, 2022, pp. 1-8.

Requisitos mínimos de concientización para usuarios de Canales Electrónicos.

Diego Sebastian Escobar.

Ciberseguridad

Requisitos mínimos de concientización para usuarios de Canales Electrónicos

Diego Sebastián Escobar

Profesor Adjunto de Tecnología de la Información. Universidad del Salvador.

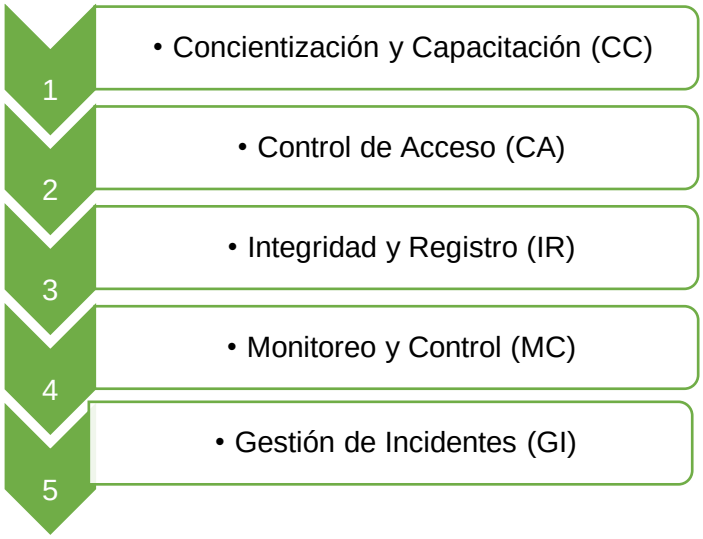
Introducción

En el año 2016, entró en vigencia la Comunicación “A” 6017 del (BCRA) la cuál modificó la Comunicación “A” 5374 del (BCRA, 2012) estableciendo nuevos requisitos y medidas a implementar en los Canales Electrónicos en donde operan los clientes de las entidades bancarias.

El objetivo principal del presente artículo es identificar los requisitos mínimos que deben contener los planes de sensibilización para profesionales en Ciencias Económicas en el rol de usuarios finales del sistema financiero argentino.

La citada norma de cumplimiento obligatorio incluye a la "Concientización y capacitación" de los empleados, clientes y proveedores dentro de los procesos específicos de los mencionados canales:

Procesos establecidos en la Comunicación "A" 6017 del BCRA



Fuente: Elaboración Propia basado en (BCRA, 2016)

Para cada uno de estos, el BCRA especifica los criterios y los procedimientos a implementar por la entidad; planteando un nuevo desafío en la gestión de la Seguridad en las entidades bancarias. La citada Comunicación establece que "*se encuentran alcanzadas las entidades financieras que intervengan en la prestación,*

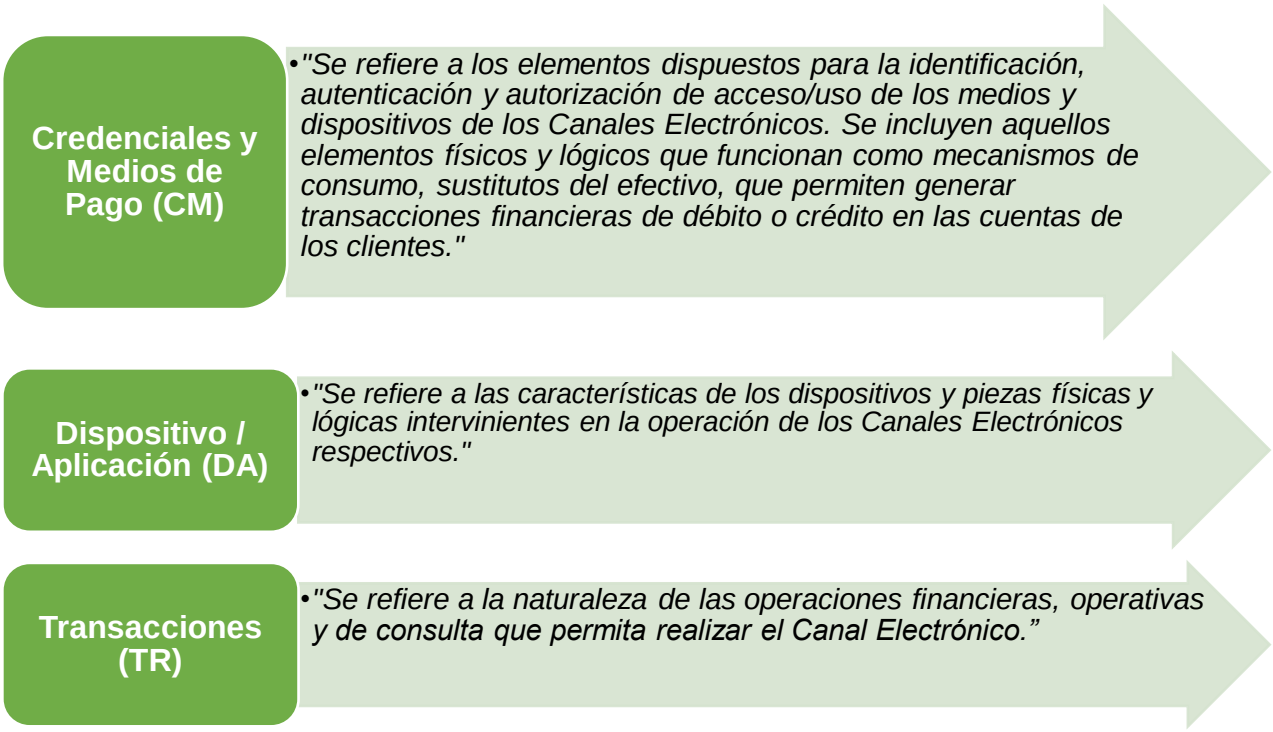
por sí o por terceros en su nombre, de servicios financieros por intermedio de algunos de los siguientes Canales Electrónicos (CE)" (BCRA, 2016).

Canales Electrónicos

Fuente: Elaboración Propia basado en (BCRA, 2016)

Además, para el análisis de cada canal se establecen los "escenarios", que están representados en tres categorías y agrupados por el mismo interés:

Escenarios en Canales Electrónicos



Fuente: Elaboración Propia basado en (BCRA, 2016)

Reflexiones finales

Teniendo en cuenta los escenarios y los canales electrónicos, resulta fundamental describir en primer lugar a los destinatarios de la concientización y capacitación dispuesta por la normativa vigente. Con ese fin, se identifica al “Cliente Externo”, con los clientes que operan por los canales electrónicos y al “Cliente Interno” con los empleados de la entidad.

Considerando todo lo expuesto, a continuación, se presentan los requisitos mínimos de Concientización y Capacitación que es exigida por la norma:

ESQUEMA N°1: Requisitos mínimos de Concientización y Capacitación

Código de requisito	Descripción de requisito
RCC001	Los contenidos del programa de CC deben formularse y mantenerse actualizados en base a un análisis de las vulnerabilidades y los resultados de la Gestión de Incidentes, e incluir, pero no limitarse a incidentes: reportados, detectados y conocidos.
RCC002	Los contenidos del programa de CC deben incluir: técnicas de detección y prevención de apropiación de datos personales y de las credenciales mediante ataques de tipo “ingeniería social”, “phishing”, “vishing” y otros de similares características.
RCC003	Los contenidos del programa de CC deben incluir: técnicas de detección y prevención del “skimming” y apropiación de datos de las credenciales mediante técnicas de intervención física.
RCC004	Los contenidos del programa de CC deben incluir: técnicas de detección de situaciones sospechosas en el recinto o entorno de acceso al CE.
RCC005	Mantener informado al personal interno, personal responsable por la gestión del CE, personal de terceros involucrado en las tareas operativas y clientes sobre las vías de comunicación para la recepción de denuncias o problemas en el circuito asociado al escenario descripto.
RCC006	Respecto de la audiencia del programa de CC, deben aplicarse los siguientes criterios: a. Características y segmentación de la audiencia, de acuerdo con el nivel de intervención en el proceso y naturaleza de la función o rol que ocupa cada participante. b. Deben encontrarse alcanzados todos los participantes necesarios en el flujo completo de la actividad indicada en el escenario. c. Orientado, pero no limitado a: personal interno, personal responsable por la gestión del CE, proveedores y clientes.

RCC007	Con una periodicidad mínima anual, debe efectuarse un análisis del Programa de CC ejecutado que mida la evolución de los incidentes, respecto de las actividades de CC realizadas incluyendo como mínimo: a. Un reporte de la cantidad y segmentación de destinatarios y contenidos del programa de CC. b. Una comparación entre los contenidos cubiertos por el programa de CC y la cantidad y tipo de incidentes de seguridad reportados/detectados/conocidos.
RCC008	Los contenidos del programa de CC deben incluir: medidas y técnicas para la protección de la privacidad de las credenciales.
RCC009	Los contenidos del programa de CC deben incluir: recomendaciones específicas sobre el uso seguro de los dispositivos propios del usuario y los dispositivos provistos por la entidad/operador.
RCC010	Los contenidos del programa de CC deben incluir: recomendaciones específicas sobre las prácticas de seguridad en la plataforma de soporte de CE.
RCC011	Los contenidos del programa de CC deben incluir: acciones específicas del usuario para la configuración de los dispositivos propios para comunicación con el CE (teléfonos, computadores personales, tabletas electrónicas, entre otros). Incluye, pero no se limita a las características diferenciadas por dispositivo para el almacenamiento de datos, reposo/bloqueo automático, eliminación de información antes del descarte o reemplazo del dispositivo, actualización de sistemas operativos y piezas de software provistas por la entidad para uso del CE.
RCC012	Los contenidos del programa de CC deben incluir técnicas específicas para el desarrollo/adquisición/fabricación, implementación, homologación y prueba de características de seguridad de los dispositivos y piezas de software provisto por la entidad/operador, asegurando que el personal involucrado interno/externo se encuentra debidamente capacitado para disminuir las fallas de implementación de las características de seguridad.
RCC013	Las entidades/operadores deben contar con un mecanismo de comunicación de los contenidos de su programa de concientización y capacitación que asegure:

	a. Que los destinatarios se encuentran continuamente informados. b. Que los destinatarios pueden efectuar consultas y evacuar dudas.
RCC014	En la selección/cambio, por parte del cliente, de los valores de los elementos de autenticación basados en el factor "algo que sabe", la entidad/operador deben recomendar al titular que los valores no se compongan al menos de: a. Una secuencia de número asociado a un dato personal público. b. Serie de caracteres o números iguales. c. Incremento o decremento de número consecutivo. d. Fechas de significación histórica.

Fuente: Comunicación "A" 6017 (BCRA, 2016)

Bibliografía

BCRA. (2016). *Comunicación "A" 6017, "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras".* Buenos Aires: Banco Central de República Argentina.

BCRA. (2012). *Comunicación "A" 5374: "Normas sobre "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras".* Buenos Aires: Banco Central de la República Argentina.

Escobar, D. S. (2010). Ley de Protección de Datos Personales. *Revista Imagen Profesional de La Federación Argentina de Consejos Profesionales en Ciencias Económicas*, 22-24.

Escobar, D. S. (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.* Buenos Aires: Facultad de Ciencias Económicas. UBA.

Escobar, D. S. (2017). Concientización y capacitación del educando en la criticidad de la información contable en el ámbito de la práctica profesional. *XXXIX SIMPOSIO DE PROFESORES DE PRÁCTICA PROFESIONAL* (págs. 40-50). San Fernando del Valle de Catamarca: UNIVERSIDAD NACIONAL DE CATAMARCA.

Villegas, M. (2008). Modelo de Madurez para la Gestión y Administración de la Seguridad Informática en las Universidades. *Trabajo de Grado para optar a la Magíster en Ingeniería de Sistemas*. Caracas, Venezuela: Universidad Simón Bolívar.

Villegas, M., Orlando, V., & Walter, B. (2009). Modelo de Madurez de la Gestión de la Seguridad Informática en el Contexto de las Organizacion es Inteligentes. *Seventh LACCEI Latin American and Caribbean Conference for Engineering and Technology, Energy and Technology for the Americas: Education, Innovation, Technology and Practice.* Venezuela: LACCEI.