MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LAINFORMACIÓN

ANÁLISIS DEL CICLO DE VIDA DE LLAVES DE CIFRADO DE CAJEROS AUTOMÁTICOS PARA ENTIDADES FINANCIERAS DEL ECUADOR

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

Magíster en Auditoría de Tecnologías de la Información

Por el estudiante:
Cristhian Fabricio SILVA ZAMBRANO

Bajo la dirección de:
Christian Mauricio MERCHÁN MILLÁN

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Junio del 2018

Análisis del ciclo de vida de llaves de cifrado de cajeros automáticos para entidades financieras del Ecuador.

Life cycle analysis of encryption keys in ATMs for financial entities in Ecuador.

Cristhian Fabricio SILVA ZAMBRANO[1]
Christian Mauricio Merchán Millán[2]

Resumen

Este artículo realiza un análisis del ciclo de vida de llaves de cifrado de cajeros automáticos para entidades financieras del Ecuador, con el objetivo de presentar recomendaciones en los procesos operativos involucrados. La norma nacional de riesgo operativo JB-2014-3066 de la Junta Bancaria del Ecuador, y la norma internacional PCI DSS, fueron utilizadas como base para elaborar una encuesta sobre el anásis del ciclo de vida de llaves de cifrado. Las entidades financieras evaluadas decidieron mantener en reserva sus nombres comerciales. El personal encuestado corresponde a departamentos de riesgo, operación de cajeros automáticos, seguridad y tecnologías de la información. Se identificó que la vulnerabilidad con mayor criticidad se encuentra en la capacitación del personal de los departamentos de operación de cajeros automáticos, riesgo y seguridad de la información. Se ha determinó como oportunidad de mejora, evaluar la pérdida de confidencialidad de las llaves de cifrado, y su impacto sobre la economía y reputación de entidades financieras. Se concluye, en base a la normativa, que las entidades financieras cumplen con requisitos mínimos de seguridad para el ciclo de vida de llaves de cifrado, sin embargo, la falta de capacitación del personal, la constante evolución de las tecnologías, y bajo nivel de compromiso de la alta administración, generan nuevos riesgos. Un factor que no se analizó en este estudio es el desempeño económico de una entidad financiera y su influencia sobre la inversión en seguridad del ciclo de vida de llaves de cifrado de cajeros automáticos.

Palabras clave: | Llaves de cifrado, seguridad, cajeros automáticos.

Abstract

This article analyzes the life cycle of ATM encryption keys for financial entities in Ecuador, with the aim of presenting recommendations on the operating processes involved. The national standard for operational risk JB-2014-3066 of the Banking Board of Ecuador, and the international standard PCI DSS, were used as a basis to prepare a survey on the analysis of the life cycle of encryption keys. The financial entities evaluated decided to keep their commercial names in reserve. The personnel surveyed correspond to risk departments, operation of ATMs, security and information technologies. It was identified that the most critical vulnerability is found in the training of personnel in the departments of operation of ATMs, risk and information security. It has been determined as an opportunity for improvement, to evaluate the loss of confidentiality of the encryption keys, and its impact on the economy and reputation of financial entities. It is concluded, based on the regulations, that financial entities comply with minimum security requirements for the life cycle of encryption keys, however, lack of staff training, the constant evolution of technologies, and low level of security. commitment of senior management, generate new risks. One factor that was not analyzed in this study is the financial performance of a financial institution and its influence on the investment in security of the life cycle of ATM encryption keys.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail csilva@uees.edu.ec.

[2] Magíster en Sistemas de Información Gerencial. Docente de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo- Ecuador.

Key words | Encryption keys, Security, ATMs.

INTRODUCCIÓN

Los sistemas transaccionales de los cajeros automáticos utilizan técnicas criptográficas para brindar servicios con estándares internacionales de confiabilidad, sin embargo, las políticas de seguridad de la información pueden estar implementadas de manera incorrecta o incompleta, ocasionando que aumente el riesgo de fraudes, fuga de información y delitos informáticos, por lo que surge la necesidad de evaluar el ciclo de vida de llaves de cifrado relacionada al servicio de cajeros automáticos (PCI Security Standards Council, 2018).

La criptografía ha utilizado técnicas de cifrado hace varios siglos, la primera técnica que se tiene conocimiento fue empleada por Damarato en el siglo VI a.C. con la intención de volver ilegible una mensaje escrito en una tablilla recubierta de cera (Núñez Contreras, L., 1994).

Con el pasar del tiempo se definieron dos técnicas de cifrado, la de transposición, inventado por los griegos, y la de sustitución, inventado en la era de la República romana (Triguero, J. J. O., Guerrero, M. Á. L., & del Castillo Crespo, E. C. G., 2005). Estos sistemas estructuran la base de lo que hoy conocemos como ciencia de criptografía (Paredes, G., 2006).

El objetivo de la criptografía es cifrar la información en medios digitales para que sean transmitidos por un emisor, a través de un canal, hacia un receptor, de manera que los caracteres o variables aleatorias contenidas en el mensaje definan el nivel de confidencialidad de acuerdo a la complejidad y repetición (Shannon, C. E., 1948). Actualmente, el método de cifrado más seguro utiliza criptografía asimétrica, por su alta complejidad requerida para resolver operaciones matemáticas de logaritmo y factorización (Kamlofsky, J., Abdel Masih, S., Colombo, H., Veiga, D., & Hecht, P., 2015) y es utilizado para proteger información almacenada en medios digitales, abarcando desde información personal hasta información que es utilizada para autorizar transacciones monetarias, por eso, es que se ha convertido en un blanco para cometer fraudes informáticos.

La Fiscalía General de España en su memoria anual 2015 estima que el 80% de los delitos informáticos está relacionado con el robo de contraseñas y datos transaccionales (ABC España, 2016). Por otra parte, el estado ecuatoriano, en los últimos diez años, ha mejorado los sistemas de gestión de seguridad informática pública (Ministerio de Finanzas del Ecuador, 2014), sin embargo, actualmente ocupa el puesto 66 de 193 países de un listado que evalúa políticas, estrategias, investigación y desarrollo de ciberseguridad (El Comercio, 2017).

La norma PCI DSS es la guía internacional de mayor prestigio para operaciones y seguridad en cajeros automáticos y tarjetas de pago, cada entidad financiera del Ecuador es responsable de cumplir esta norma bajo la supervisión de la Red Nacional de Cajeros Automáticos, asimismo la Junta Bancaria del Ecuador, mediante resolución JB-2014-3066 del año 2014 recomienda realizar auditorías externas con consultores especializados, así como mantener actualizados los procedimientos de cifrado de acuerdo al estándar de la industria internacional (Superintendencia de Bancos del Ecuador, 2014).

Estas recomendaciones tienen como objetivo mejorar la seguridad de los procesos asociados al ciclo de vida de llaves de cifrado de cajeros automáticos, gestionar las vulnerabilidades de activos de información y procesos relacionados (Monsalve-Pulido, J. A., Aponte-Novoa, F. A., & Chaves-Tamayo, D. F., 2014). Así que nos encontramos ante un desafío que gestionado, según la normativa mencionada en el párrafo anterior, permitirá a las entidades financieras tomar medidas correctivas en el ciclo de vida de llaves de cifrado de cajeros automáticos para evitar pérdidas económicas (León, V. C., 2004)

El objetivo del presente estudio es analizar el ciclo de vida de llaves de cifrado de cajeros automáticos de las entidades financieras del Ecuador, para proponer acciones que permitan eliminar, mitigar, transferir o aceptar los riesgos (Del Carpio, J., 2006).

Para cumplir con el objetivo se realizó una encuesta, mediante formularios web, a entidades financieras propietarias de cajeros automáticos del Ecuador. Luego se aplicó la norma ISO 31000:2009 para realizar el proceso de gestión del riesgo: con los resultados de la encuesta se identificaron vulnerabilidades en el ciclo de vida de llaves de cifrado de cajeros automáticos, de acuerdo a su probabilidad e impacto, se determinó el nivel de riesgo para cada vulnerabilidad. Con esta información clasificada y ponderada se procedió a realizar las recomendaciones y oportunidades de mejora en concordancia con la norma nacional de la Junta Bancaria y la norma internacional PCI DSS (Purdy, G., 2010).

La encuesta realizada ha sido un instrumento metodológico que ha permitido evaluar el ciclo de vida de llaves de cifrado de cajeros automáticos, los resultados permitieron determinar niveles de riesgo y oportunidades de mejora de las brechas encontradas en el ciclo de vida de llaves de cifrado de cajeros automáticos de las entidades financieras del Ecuador. Las entidades financieras podrán establecer planes de acción para evitar multas y sanciones por parte de los organismos de control (Superintendencia de Bancos del Ecuador, 2014).

MARCO TEÓRICO

CAJEROS AUTOMÁTICOS

Los cajeros automáticos son dispositivos que tienen como objetivo brindar servicios transaccionales a clientes de entidades financieras mediante una tarjeta plástica (Cambridge University Press, 2018). El funcionamiento operativo es el siguiente: el cliente se acerca con su tarjeta plástica al cajero automático, la introduce en una ranura, y procede a digitar su clave, cumpliendo así con la autenticación segura, que consiste en cumplir como mínimo dos de los siguientes tres factores: algo que se tiene, algo que se sabe o algo que se es (Liu, S., & Silverman, M., 2001).

Además, se estima que para el año 2023 todos los cajeros automáticos aceptarán tecnología *contactless*, es decir, el usuario pasará la tarjeta, el mando o el teléfono móvil por delante del dispositivo como parte del mecanismo de autenticación de la transacción, y será opcional introducir la tarjeta en la ranura del cajero automático como se realiza actualmente (NFC World, 2018).

PCI DSS

PCI-DSS, *PaymentCardIndustry Data Security Standard* por sus siglas en inglés, es una norma internacional de seguridad para la industria de tarjetas de pago y cajeros automáticos, soportadas por *PCI Security Standards Council*, organismo implementado con la finalidad de desarrollar, difundir, mejorar y ayudar en la adopción de estándares de seguridad para la industria de tarjetas de pago y cajeros automáticos (PCI Security Standards Council, 2018).

ISO/IEC 27001:2013

Es un estándar certificable y auditable que provee un modelo para establecer, implementar, operar, monitorear, mantener y mejorar un Sistema de Gestión de Seguridad de la Información, que realiza un enfoque metodológico para administración de información sensible. Propone un proceso de mejora continua para proteger la integridad, disponibilidad y confidencialidad, de la información; incluye a empleados, procesos y sistemas informáticos (ISO/IEC 27001:2013).

ISO 31000:2009

Es un estándar desarrollado por comités internacionales integrados por miembros con experiencia comprobable en procesos de gestión de riesgos (International Organization for

Standardization, 2009). A continuación se muestra un gráfico que resume el proceso de administración del riesgo:

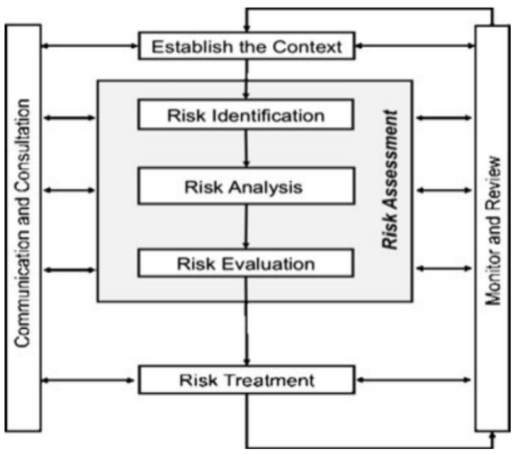


Figura 1.- Procesos de administración de riesgo de ISO 3100:2009 (Purdy, G., 2010).

El proceso de administración de riesgo establece los principales pasos a seguir para identificar, analizar, evaluar (impacto y magnitud) y dar tratamiento a los riesgos y vulnerabilidades (Leitch, M., 2010).

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (S.G.S.I.)

S.G.S.I. tiene como objetivo identificar los riesgos de seguridad de la información para que sean conocidos, minimizados y gestionados de forma sistemática, documentada, eficiente, repetible, estructurada de forma que se adapte a los cambios que se realicen en el entorno y tecnologías (ISO/IEC 27001:2013).

Dentro de los procedimientos de gestión de S.G.S.I. encontramos: Planear (políticas, objetivos y alcance, inventario de activos, análisis de riesgos), implementar (Políticas y procedimientos), auditar y revisar (auditoría de verificación), análisis de riesgo, mantener y mejorar (Acciones correctivas y preventivas), evaluación de riesgos (determinar la importancia del riesgo de acuerdo a los criterios de la entidad), tratamiento de riesgos (procedimientos para eliminar, minimizar, asumir y transferir riesgos (ISO 27000.es, 2014).

CRIPTOGRAFÍA

La criptografía se refiere a la escritura secreta (Kahn, D., 1996), que minimiza la divulgación del contenido que se encuentra cifrado, controles de acceso y firma digital de documentos (Diffie, W., & Hellman, M. E., 1976).

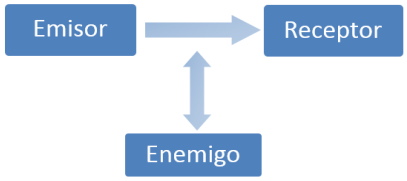


Figura 2.- Interceptación de las comunicaciones entre el emisor y el receptor (Giménez, V. M., 2011).

En la Figura 2 se puede visualizar la comunicación entre el emisor y receptor, un tercero ubicado en medio del canal de comunicación intenta acceder a la información transmitida a través de mecanismos que le permitan conocer su contenido, si esta información no está cifrada el atacante tendrá acceso a la misma (Buchmann, J., 2013).

La criptografía se divide en tres ramas principales:

Algoritmos simétricos: Fue el principal mecanismo de cifrado desde la antigüedad hasta el año 1976 donde dos partes comparten una llave secreta para cifrar y descifrar un mensaje, en la actualidad se utiliza para verificar la integridad de un mensaje y para cifrar datos (Paar, C., & Pelzl, J., 2009)

Algoritmos asimétricos: Al igual que en la criptografía simétrica un usuario tiene una clave secreta y una clave pública, puede ser utilizado para firmas digitales, claves, y cifrado de datos (Hellman, M. E., 1979).

Protocolos Criptográficos: Trata sobre la aplicación de algoritmos simétricos, asimétricos y funciones hash para comunicación segura en internet, presente en algoritmos TLS en navegadores web (Ayuso, J. G. T., 2003).

Una de las implementaciones más importantes de la criptografía es la clave pública que provee

autenticación, por ejemplo de firmas digitales para autenticación de mensajes y no repudio, el sistema almacena la clave pública para que la acción se ejecute si la firma digital ha sido verificada (Galbraith, S. D., 2012).

La principal dificultad para desarrollar sistemas basados en criptografía de clave pública es el despliegue y administración de infraestructuras para soportar la autenticidad de claves criptográficas: proveer y garantizar la relación entre la clave pública y la autoridad de la clave privada, ésta garantía es entregada en un certificado o una firma de la autoridad de certificación de una clave pública (Al-Riyami, S. S., & Paterson, K. G., 2003).

ETHICAL HACKING

Los ataques informáticos que ocurren en internet explotan vulnerabilidades simultáneamente. Las pruebas conceptuales y laboratorio de *Computer Emergency Response Team* (CERT) demuestran las características más vulnerables de aplicaciones, páginas y accesos web: Autenticación débil, privilegio excesivo, vulnerabilidad de archivos, ejecución inducida (Smith, R. E., 1995).

Las vulnerabilidades web descritas en el párrafo anterior fueron planteadas hace veinte años aproximadamente; son enunciados cortos pero precisos si los comparamos con el TOP 10 de Open Web Application Security Project, abreviado *OWASP,* que es el documento más utilizado hoy en día (Jin, X., Hu, X., Ying, K., Du, W., Yin, H., & Peri, G. N., 2014) para analizar los riesgos más críticos de seguridad para aplicaciones web: *Injection, Broken Authentication and Session Management, Cross-Site Scripting (XSS), Insecure Direct Object References, Security Misconfiguration, Sensitive Data Exposure, Missing Function Level Access Control, Cross-Site Request Forgery (CSRF), Using Known Vulnerable Components, Unvalidated Redirects and Forwards* (OWASP, T., 2013).

OWASP

OWASP plantea una metodología para realizar test de intrusión, análisis de riesgos y medición de impacto a la seguridad de la información de aplicaciones web priorizando la gestión de las vulnerabilidades, sobre el modelo de defensa en profundidad solamente explica que se implementan varias capas de seguridad donde la información principal del negocio sea el núcleo con mayor protección, sin embargo no plantea una arquitectura de seguridad informática (Kenan, K., 2006).

NIST SP800-115

NIST SP800-115 es una guía técnica para pruebas y evaluación de seguridad de la información, puede usarse para varios objetivos (National Institute of Standards and Technology, 2008), como identificar vulnerabilidades en un sistema de red y analizar el cumplimiento de políticas o procedimientos, porque en caso de existir vulnerabilidades en los aplicativos o sistemas operativos podría ocurrir que un atacante logre su cometido y genere pérdidas económicas a clientes o entidades financieras (Lippmann, R., Ingols, K., Scott, C., Piwowarski, K., Kratkiewicz, K., Artz, M., & Cunningham, R., 2006).

ADMINISTRACIÓN DE LLAVES DE CIFRADO DE CAJEROS AUTOMÁTICOS

En una transacción de cajeros automáticos ó ATM en sus siglas en inglés, pueden intervenir hasta 3 (tres) entidades financieras:

- Entidad financiera propietaria del cajero automático
- Entidad financiera emisora de tarjeta plástica
- Red de cajeros automáticos.

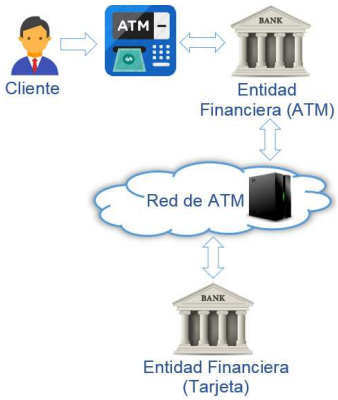


Figura 3.- Transacción en cajero automático con intervención de diferentes entidades financieras.

Para realizar una transacción de cajero automático se debe establecer la comunicación con una llave pública compartida (PK) que será custodiada por cada una de las entidades involucradas. Sin embargo el ciclo de vida de las llaves de cifrado utilizadas, para autorizar al cajero automático, es gestionada por la entidad propietaria del mismo (PCI Security Standards Council., 2018).

Generación de la llave

La entidad propietaria del cajero automático utiliza un servidor de propósito específico denominado HSM *ó hardware security module*, para generar una llave pública, compuesta de 16 dígitos alfanuméricos. Esta llave es registrada en un medio físico, y se almacena en una bóveda hasta que el cajero automático se implemente en producción, fecha en la cual es entregada al responsable de operación del cajero automático, en este registro se incluye un identificador único que es compartido entre entidades para determinar la correspondencia entre llave y cajero automático (Al-Vahed, A., & Sahhavi, H., 2011).

Asignación de custodio

La llave y su identificador único es entregada, mediante un acta de entrega, al responsable de operación del cajero automático en calidad de custodia (ISO/IEC 27001:2013).

Figura 4.- El operador del cajero automático recibe la clave.

La llave podrá ser solicitada al operador en caso de mantenimiento o auditorías informáticas internas, por personal de la entidad financiera propietaria del cajero automático (Zheng, Y., & Imai, H., 1998).

Registro

El operador registra la llave y el identificador único en el cajero automático y en la Red de cajeros automáticos, ambos realizan validaciones para determinar que la llave cuenta con la fortaleza mínima sugerida por NIST y OWASP para cumplimiento del mandato del estándar internacional de cajeros automáticos y tarjetas de pago (PCI Security Standards Council., 2018).

Figura 5.- El operador de la entidad financiera registra la llave en el cajero automático y en la red de cajeros.

Actualización

La entidad financiera propietaria del cajero automático reemplaza las llaves anualmente: cada nueva llave es generada, asignada al custodio, y, registrada para cada uno de los cajeros automáticos y en la red de cajeros automáticos (Superintendencia de Bancos del Ecuador, 2014).

Figura 6.- Un funcionario de la entidad financiera registra la nueva llave en el cajero automático y en la red de cajeros.

Se realizan pruebas para certificar que el sistema funciona correctamente, el operador del cajero automático entrega la llave caducada a la entidad financiera propietaria del cajero automático (BANRED, 2015).

METODOLOGÍA

La metodología seleccionada en el desarrollo del presente artículo corresponde al esquema de procesos de administración de riesgo, que cumple con los requisitos de la norma internacional PCI DSS y la resolución JB-2014-3066 de la Junta Bancaria del Ecuador, y permite identificar vulnerabilidades en orden de probabilidad e impacto, determinar niveles de riesgo para cada vulnerabilidad, establecer recomendaciones y oportunidades de mejora (Tummala, R., & Schoenherr, T., 2011).

Estudiar el ciclo de vida (Generación, custodia, registro y actualización) de llaves de cifrado de cajeros automáticos de las entidades financieras del Ecuador. Analizar los resultados de la encuesta elaborada por el autor del presente artículo. La encuesta fue elaborada según la *Sección VII, Título X, Capítulo V del Libro I de las Normas generales para la aplicación de la ley general de instituciones del sistema financiero* (Superintendencia de Bancos del Ecuador, 2014), y en la norma internacional *PCI DSS v3.2*.

En el Anexo 3 del presente artículo, se justifica la selección de los literales de las normativas mencionadas que fueron utilizados para elaborar la encuesta y análisis (ISO 9001:2015) del ciclo de vida de llaves de cifrado en cajeros automáticos.

En el Anexo 4 se presenta evidencia de todas las encuestas resueltas, pero para mantener la confidencialidad de los encuestados se les asignó un código de identificación bajo custodia del autor.

Identificar vulnerabilidades en el proceso de gestión de ciclo de vida de llaves de cifrado de cajeros automáticos con la finalidad de mantener estándares de seguridad en las transacciones de cajeros automáticos sobre todo en las que intervienen dos entidades financieras.

Establecer recomendaciones que permitan realizar un tratamiento de riesgo de las vulnerabilidades del ciclo de vida de llaves de cifrado de cajeros automáticos.

Alcance de la Investigación

Descriptiva: Con el objetivo de realizar un análisis de vulnerabilidad, se realizará, en un anexo, el cálculo del nivel de riesgo, que será calculado en base a la probabilidad e impacto de las brechas identificadas en los resultados de la encuesta. Una vez obtenido el nivel de riesgo de cada vulnerabilidad, éstas se ordenarán, en otro anexo, de acuerdo al nivel de criticidad, y se elaborará un plan de acción, estableciendo las recomendaciones y responsables de ejecutar las mejoras correspondientes.

Unidad de análisis

Por motivo de confidencialidad se mantendrá en secreto el nombre de las entidades financieras, la información base se obtendrá mediante la revisión de encuestas, estadísticas, libros, internet, normativa, leyes para entidades financieras nacionales e internacionales.

Actualmente existen 20 (veinte) entidades que son propietarias de cajeros automáticos (Banred, 2018).

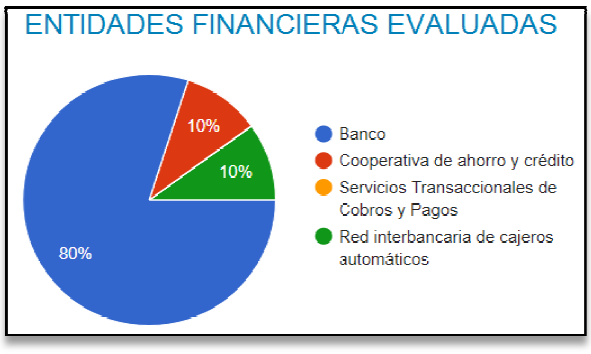


Figura 7.- Entidades financieras evaluadas (muestra)

Se ha encuestado a 10 (diez) colaboradores de 4 (cuatro) entidades financieras, que corresponden al 20% del universo, distribuido de acuerdo a la Figura 7 del presente artículo.

ANÁLISIS DE RESULTADOS

Simbología

Se identifica con color rojo al riesgo alto, amarillo al riesgo medio, y verde al riesgo bajo:

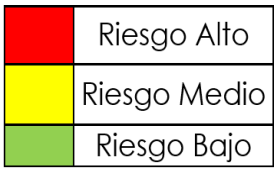


Figura 8.- Identificación del riesgo

Matriz de riesgo

Como resultado de la evaluación de riesgo se obtuvo la siguiente matriz:

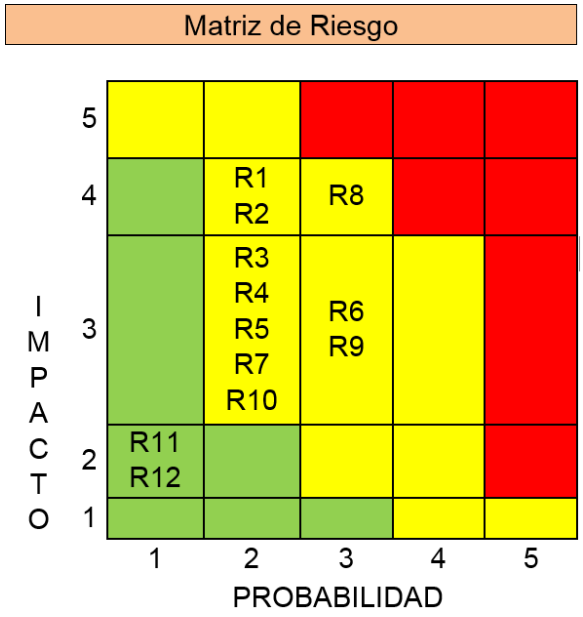


Figura 9.- Matriz de Riesgo

A continuación se explica la matriz de riesgo y los ítems identificados como riesgo medio:

R8: Falta de capacitación al personal de operación de cajeros automáticos

La resolución *JB-2014-3066,* de la Junta Bancaria del Ecuador y la norma internacional PCI DSS v3.2, recomiendan, a las entidades financieras, realizar capacitaciones al personal de operación de cajeros automáticos con el objetivo de reducir riesgos informáticos, operativos y financieros; sin embargo los resultados de la encuesta determinan que no se ha cumplido según lo sugerido, tal como se muestra a continuación:

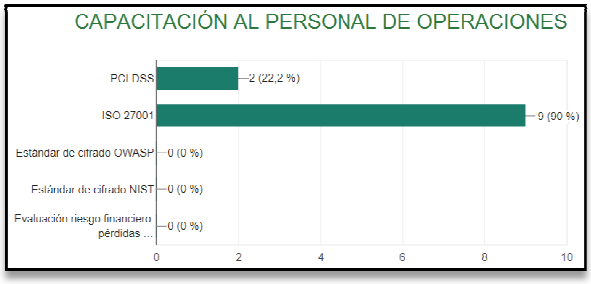


Figura 10.- Capacitación a personal de operaciones.

Según los resultados de la encuesta, la mayoría de las entidades financieras cumplen con capacitación al personal de operaciones de cajeros automáticos, sobre temas de ISO 27001:2013, sin embargo, existe una deficiencia de capacitación sobre temas de PCI DSS, riesgo financiero, OWASP y NIST.

La función de los operadores de cajeros automáticos es custodiar llaves de cifrado y realizar diariamente actividades operativas relacionadas a cajeros automáticos. La resolución *JB-2014-3066,* de la Junta Bancaria del Ecuador, indica que se deben utilizar estándares internacionales de la industria como PCI DSS, OWASP y NIST, que no han sido incluidas en el proceso de capacitación porque las entidades no han implementado procesos, procedimientos completos de seguridad bancaria, fraudes informáticos y seguridad de la información; según las entrevistas personales, esto se debe a falta de presupuesto y a la crisis económica que ha venido atravesando el país en los últimos diez años (BBC Mundo, 2017).

Con el objetivo de cumplir la normativa *JB-2014-3066* y PCI DSS v3.2, el área de seguridad de la información, así como dirección y gerencia son

responsables de desarrollar manuales de procedimientos e implementar procesos formales para capacitar al personal de operaciones de cajeros automáticos para mejorar la seguridad del ciclo de vida de llaves de cifrado.

R1: Dificultad para determinar las pérdidas económicas y niveles de reputación originadas por la pérdida de confidencialidad de las llaves de cifrado.

La resolución *JB-2014-3066,* de la Junta Bancaria del Ecuador y la norma internacional PCI DSS v3.2, recomiendan, a las entidades financieras, realizar auditorías externas que analicen y recomienden acciones que permitan reducir riesgos informáticos, operativos y financieros; sin embargo, según los resultados de la encuesta, las entidades financieras no han incluido, en las auditorías, la evaluación del impacto económico de los riesgos informáticos o los riesgos de fraudes que puedan ser cometidos por personal de servicio al cliente, operativo, clientes o intrusos:

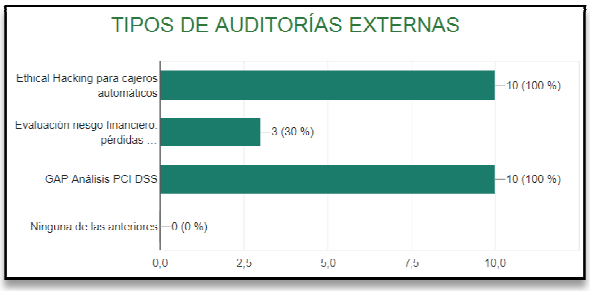


Figura 11.- Tipos de auditorías externas.

Según los resultados de la encuesta, todas las entidades financieras realizan las auditorías Ethical hacking, y GAP Análisis PCI DSS, sin embargo, solo una tercera parte de las entidades financieras ha realizado Evaluación de riesgo financiero, pérdidas económicas y niveles de reputación.

Con el objetivo de cumplir la normativa *JB-2014-3066* y PCI DSS v3.2, el área de seguridad de la información, así como dirección y gerencia son responsables de desarrollar manuales de procedimientos, implementar procesos formales y segregados para la contratación de auditorías externas.

R10: Falta de capacitación a dirección y gerencia

La resolución *JB-2014-3066,* de la Junta Bancaria del Ecuador y la norma internacional PCI DSS v3.2, recomienda realizar capacitaciones al personal responsable de la dirección y gerencia de las entidades financieras, sin embargo los resultados de la encuesta determinan que no se ha cumplido según lo sugerido, tal como se de muestra a continuación:

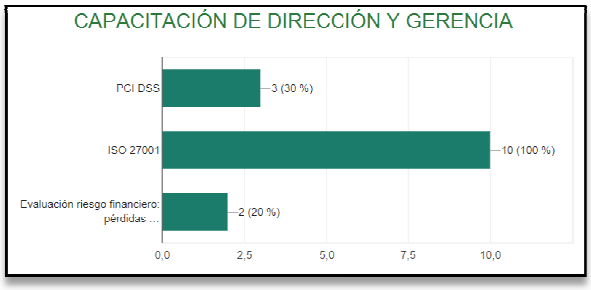


Figura 12.- Capacitación de gerencia y alta dirección.

Según los resultados de la encuesta, todas las entidades financieras cumplen con capacitación sobre ISO 27001 a personal de gerencia y alta dirección, sin embargo, falta capacitarlos sobre PCI DSS y Evaluación de riesgo financiero.

Con el objetivo de cumplir la normativa *JB-2014-3066* y PCI DSS v3.2, el área de seguridad de la información, así como gerencia y dirección, son responsables de desarrollar manuales de procedimientos, implementar procesos formales de capacitación. Estas acciones soportan la toma de decisiones, innovación, por ejemplo, tecnología *contactless* (EMVCo, 2016).

R2: El proceso de administración de llaves de cifrado carece de procesos segregados y formales.

La resolución *JB-2014-3066,* de la Junta Bancaria del Ecuador y la norma internacional PCI DSS v3.2, recomienda que el proceso de administración de llaves de cifrado tenga

funciones segregadas y formales, sin embargo los resultados de la encuesta determinan que no se ha cumplido según lo sugerido, tal como se de muestra a continuación:

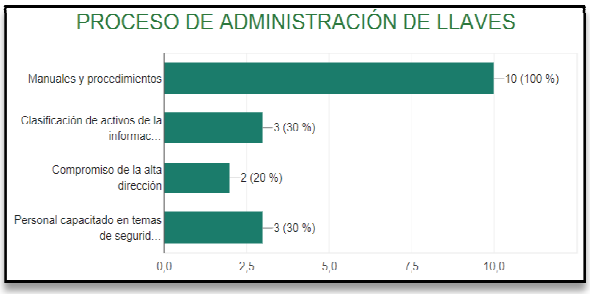


Figura 13.- Proceso de administración de llaves

Según los resultados de la encuesta, todas las entidades financieras cumplen con manuales y procedimientos de administración de llaves de cifrado, sin embargo, los procesos de clasificación de activos de información, compromiso de alta dirección, capacitación de temas de seguridad se han implementado en 30%, o menos, de las entidades financieras.

Con el objetivo de cumplir la normativa *JB-2014-3066* y PCI DSS v3.2, el área de seguridad de la información, así como dirección y gerencia son responsables de desarrollar manuales de procedimientos, implementar procesos formales y segregados de administración de llaves de cifrado.

R3: El proceso de asignación de custodio de llaves de cifrado carece de procesos segregados y formalmente asignados.

La resolución *JB-2014-3066,* de la Junta Bancaria del Ecuador y la norma internacional PCI DSS v3.2, recomienda que el proceso de asignación de custodio de llaves de cifrado tenga funciones segregadas y formales, sin embargo los resultados de la encuesta determinan que no se ha cumplido según lo sugerido, tal como se muestra a continuación:

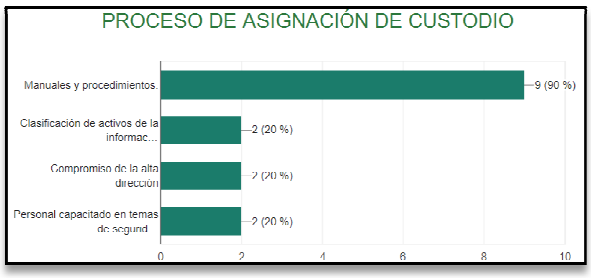


Figura 14.- Proceso de asignación de custodio.

Según los resultados de la encuesta, la mayoría de las entidades financieras cumplen con manuales y procedimientos de asignación de custodio de llaves de cifrado, sin embargo, se ha implementado encuestadas, procesos de clasificación de activos de información, compromiso de alta dirección, capacitación de temas de seguridad, en 20% de las entidades financieras.

Con el objetivo de cumplir la normativa *JB-2014-3066* y PCI DSS v3.2, el área de seguridad de la información, así como dirección y gerencia son responsables de desarrollar manuales de procedimientos, implementar procesos formales y segregados de asignación de custodio de llaves de cifrado.

R4: El proceso de registro de llaves de cifrado carece de procesos segregados y formales.

La resolución *JB-2014-3066,* de la Junta Bancaria del Ecuador y la norma internacional PCI DSS v3.2, recomienda que el proceso de registro de llaves de cifrado tenga funciones segregadas y formales, sin embargo los resultados de la encuesta determinan que no se ha cumplido según lo sugerido, tal como se de muestra a continuación:

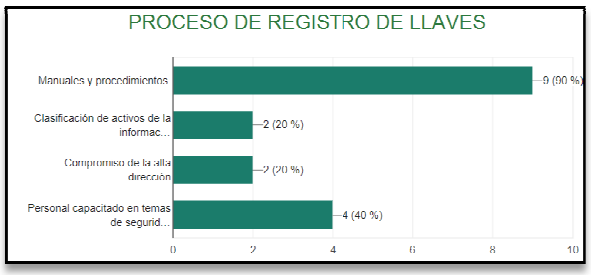


Figura 15.- Proceso de registro de llaves.

Según los resultados de la encuesta, las entidades financieras cumplen con manuales y procedimientos de registro de llaves de cifrado, sin embargo, se ha implementado en 40%, o menos, de las entidades financieras, procesos de clasificación de activos de información, compromiso de alta dirección, capacitación de temas de seguridad.

Con el objetivo de cumplir la normativa *JB-2014-3066* y PCI DSS v3.2, el área de seguridad de la información, así como dirección y gerencia son responsables de desarrollar manuales de procedimientos, implementar procesos formales y segregados de registro de llaves de cifrado.

R5: El proceso de actualización de llaves de cifrado carece de procesos segregados y formales.

La resolución *JB-2014-3066,* de la Junta Bancaria del Ecuador y la norma internacional PCI DSS v3.2, recomienda que el proceso de actualización de llaves de cifrado tenga funciones segregadas y formales, sin embargo los resultados de la encuesta determinan que no se ha cumplido según lo sugerido, tal como se de muestra a continuación:

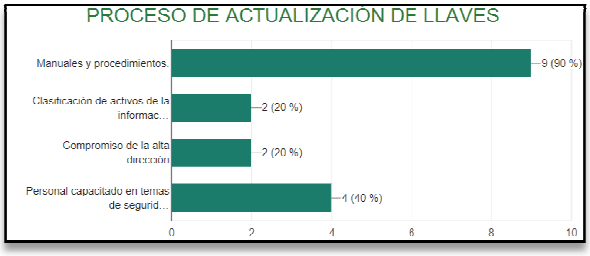


Figura 16.- Proceso de actualización de llaves.

Según los resultados de la encuesta, las entidades financieras cumplen con manuales y procedimientos de actualización de llaves de cifrado, sin embargo, se ha implementado en 40%, o menos, de las entidades financieras, procesos de clasificación de activos de información, compromiso de alta dirección, capacitación de temas de seguridad.

Con el objetivo de cumplir la normativa *JB-2014-3066* y PCI DSS v3.2, el área de seguridad de la información, así como dirección y gerencia son responsables de desarrollar manuales de procedimientos, implementar procesos formales y segregados de actualización de llaves de cifrado.

R6: Falta de capacitación al personal de seguridad de la información

La resolución *JB-2014-3066,* de la Junta Bancaria del Ecuador y la norma internacional PCI DSS v3.2, recomiendan implementar procesos de capacitación al personal de seguridad de la información, sin embargo los resultados de la encuesta determinan, que no se ha cumplido según lo sugerido, tal como se muestra a continuación:

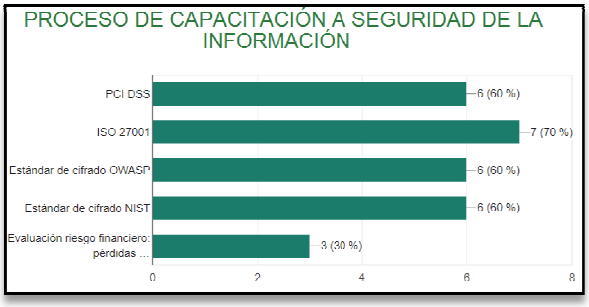


Figura 17.- Proceso de capacitación al personal de seguridad de la información.

Según los resultados de la encuesta la mayoría de las entidades financieras encuestadas realizan capacitaciones, al personal de seguridad de la información, sobre ISO 27001:2013, OWASP y NIST, y solamente una tercera parte realiza capacitaciones sobre evaluaciones de riesgo financiero.

La dirección y gerencia de las entidades financieras son responsables de asegurar que se capacite al personal de seguridad de la información en los temas mencionados en la encuesta.

Con el objetivo de cumplir la normativa *JB-2014-3066* y PCI DSS v3.2, el área de seguridad de la información, así como recursos humanos, dirección y gerencia son responsables de

desarrollar manuales de procedimientos e implementar procesos de capacitación sobre los temas indicados en la encuesta, lo que permitirá tener conocimiento para disminuir riesgos y gestionar el ciclo de llaves de cifrado de manera formal.

R7: Falta de capacitación al personal de seguridad informática

La resolución JB-2014-3066, de la Junta Bancaria del Ecuador y la norma internacional PCI DSS v3.2, recomiendan implementar procesos de capacitación al personal de seguridad informática, sin embargo los resultados de la encuesta determinan, que se ha cumplido parcialmente lo sugerido, tal como se muestra a continuación:

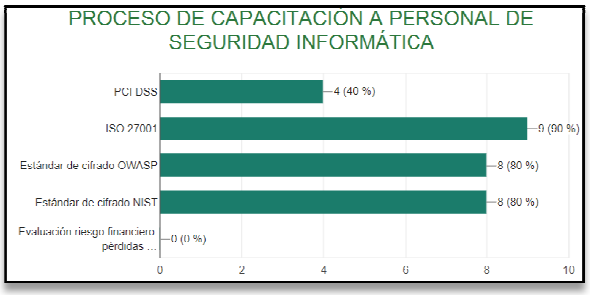


Figura 18.- Capacitación a personal de seguridad informática.

Según los resultados de la encuesta, la mayoría de las entidades financieras realizan capacitaciones, al personal de seguridad informática, sobre ISO 27001:2013, OWASP y NIST, y solamente una tercera parte realiza capacitaciones sobre evaluaciones de riesgo financiero.

La dirección y gerencia de las entidades financieras son responsables de asegurar que se capacite al personal de seguridad de la información en los temas mencionados en la encuesta.

Con el objetivo de cumplir la normativa *JB-2014-3066* y PCI DSS v3.2, el área de seguridad de la información, así como recursos humanos, dirección y gerencia son responsables de desarrollar manuales de procedimientos e implementar procesos de capacitación sobre los temas indicados en la encuesta, lo que permitirá tener conocimiento para disminuir riesgos y gestionar el ciclo de llaves de cifrado de acuerdo a lo solicitado por la normativa.

R9: Falta de capacitación al personal de riesgo

La resolución JB-2014-3066, de la Junta Bancaria del Ecuador y la norma internacional PCI DSS v3.2, recomiendan implementar procesos de capacitación al personal de riesgo, sin embargo los resultados de la encuesta determinan, que se ha cumplido parcialmente lo sugerido, tal como se muestra a continuación:

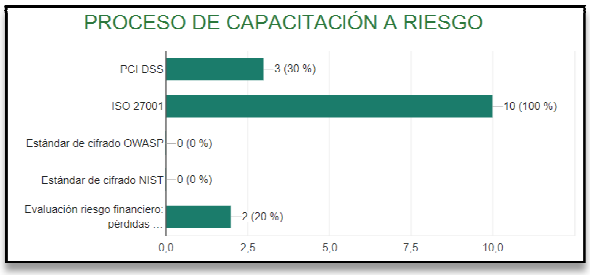


Figura 19.- Capacitación a personal de riesgo.

Según los resultados de la encuesta, las entidades financieras realizan capacitaciones, al personal de riesgo, sobre ISO 27001:2013, sin embargo menos del 30% de las entidades financieras realiza capacitaciones sobre PCI DSS y evaluaciones de riesgo financiero. Ninguna entidad financiera capacita a su personal de riesgo sobre fundamentos básicos de OWASP y NIST.

La dirección y gerencia de las entidades financieras son responsables de asegurar que se capacite al personal de riesgo en los temas mencionados en la encuesta.

Con el objetivo de cumplir la normativa *JB-2014-3066* y PCI DSS v3.2, el área de seguridad de la información, así como recursos humanos, dirección y gerencia son responsables de desarrollar manuales de procedimientos e implementar procesos de capacitación sobre los temas indicados en la encuesta, lo que permitirá

tener conocimiento para disminuir riesgos y gestionar el ciclo de llaves de cifrado de acuerdo a lo solicitado por la normativa.

Riesgo bajo

Los siguientes procesos corresponden a riesgos que pueden ser aceptados por las entidades financieras, porque no forman parte de la recomendación de la normativa, sin embargo, se considera que ayudará a mejorar la seguridad y reputación de la entidad.

R11: Falta de certificación técnica internacional de proveedores

El proceso de certificación técnica internacional de proveedores cumple casi en su totalidad con todos las certificaciones tal como se muestra a continuación:

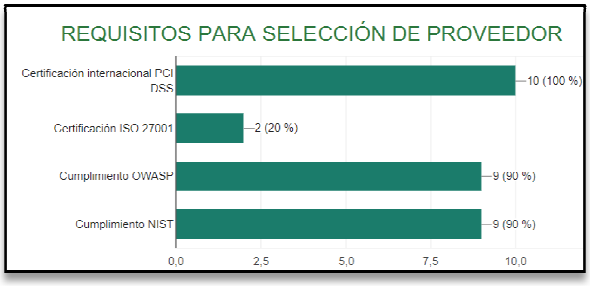


Figura 20.- Requisitos para selección de proveedor.

La certificación ISO 27001:2013 no es una exigencia para los proveedores involucrados en el ciclo de vida de llaves de cifrado de cajeros automáticos de entidades financieras del Ecuador, por lo tanto es un riesgo que se puede aceptar.

La certificación PCI DSS, cumplimiento OWASP y NIST son requisitos que se están cumpliendo satisfactoriamente para la selección de proveedores, sin embargo, es necesario realizar un proceso de monitoreo periódico para que estos indicadores no disminuyan sino que se mantengan.

R12: Falta de certificación técnica internacional de hardware y software

El proceso de certificación técnica internacional de hardware y software cumple casi en su totalidad con las certificaciones, tal como se muestra a continuación:

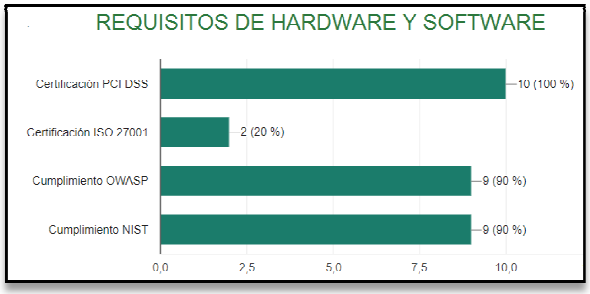


Figura 21.- Requisitos de hardware y software.

La certificación ISO 27001:2013 no es una exigencia para hardware y software relacionado al ciclo de vida de llaves de cifrado de cajeros automáticos de entidades financieras del Ecuador, por lo tanto es un riesgo que se puede aceptar.

La certificación PCI DSS, cumplimiento OWASP y NIST son requisitos que se están cumpliendo satisfactoriamente para la selección de proveedores, sin embargo, es necesario realizar un proceso de monitoreo periódico para que estos indicadores, como mínimo, se mantengan.

CONCLUSIONES

Las llaves de cifrado son generadas por el área de seguridad de la información y entregadas al área de operación de cajeros automáticos, sin embargo esta última área no ha sido capacitada de acuerdo a los requisitos de la normativa nacional de la Junta Bancaria, ni de normativa internacional PCI DSS, por lo que se debe realizar un plan de capacitación que incluya temas de seguridad operativa para criptografía de cajeros automáticos.

Este estudio se puede complementar con la realización de una guía de capacitación que incluya detalles de los temas a ser abordados por el personal de operación de cajeros automáticos para disminuir los riesgos operativos del ciclo de vida de llaves de cifrado.

Se identificó que el mayor nivel de riesgo del ciclo de vida de llaves de cifrado de cajeros automáticos se encuentra en el proceso de capacitación al personal operaciones, así como también al personal de riesgo, seguridad, dirección y gerencia, el sustento de esta afirmación se obtuvo mediante un análisis que se encuentra publicado en el Anexo 5 del presente estudio, que corresponde al análisis de las respuestas de la encuesta según la normativa PCI DSS.

Se identificó que no se cuenta con parámetros para evaluar el impacto económico que tendría la ejecución de un fraude originado por pérdida de confidencialidad en el ciclo de vida de llaves de cifrado.

La encuesta fue resuelta por personal de bancos, cooperativas de ahorro y crédito, y redes transaccionales, teniendo como limitación la reserva de los nombres de las entidades financieras evaluadas, porque estas consideraron que la información, a pesar de que no es confidencial, puede ser utilizada por terceros para fines comerciales.

El aporte del autor corresponde, basado en la normativa internacional PCI DSS, en identificar la falta de una recomendación formal y explícita del ciclo de vida de llaves de cifrado de cajeros automáticos, en la normativa legal de los organismos de control de las entidades financieras a nivel nacional. Por lo tanto, con el objetivo de mejorar la confianza y seguridad de los cajeros automáticos a nivel nacional, se sugiere tomar en consideración lo propuesto en este párrafo.

Con el objetivo de realizar nuevas investigaciones se sugiere estudiar el impacto económico que tiene la fuga de información de llaves de cifrado para cajeros automáticos, también se puede realizar una plantilla de revisión para auditoría de administración de ciclo de vida de llaves de cifrado de cajeros automáticos, de acuerdo a los siguientes literales de la normativa PCI DSS: 2.4.b (inventario actualizado), 2.5 (procedimientos operativos), 3.4.1.b (verificar que las claves criptográficas se almacenen de forma segura), 3.5 (políticas y procedimientos de administración de claves y verifique que se hayan especificado los procesos que protegen las claves utilizadas para cifrar los datos), 3.5.1 (Restrinja el acceso a las claves a la menor cantidad de custodios), 3.5.3 (Revise las ubicaciones de almacenamiento de claves), 8.4.c (conocimiento de procedimientos y las políticas de autenticación), 12.4.b (conocimiento de las políticas de seguridad), 12.6.1.c (capacitación de concienciación), 12.10.3 (respuesta a incidentes operativos).

Referencias Bibliográficas

ABC España. (2016). Más del 80 por ciento de los delitos informáticos de 2015 fueron fraudes en la Red. ABC.es. Obtenido de: https://www.abc.es/espana/abci-mas-80-ciento-delitos-informaticos-2015-fueron-fraudes-201609052138_noticia.html

Al-Vahed, A., & Sahhavi, H. (2011). An overview of modern cryptography. World Applied Programming, 1(1), 55-61.

Al-Riyami, S. S., & Paterson, K. G. (2003). Certificateless public key cryptography. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 452-473). Springer, Berlin, Heidelberg.

Ayuso, J. G. T. (2003). Protocolos criptográficos y seguridad en redes. Ed. Universidad de Cantabria.

BANRED. (2015). Guía de uso Tecnología EMV. Banred.fin.ec. Obtenido de: https://www.banred.fin.ec/imagesFTP/7757.EMV_BANRED.pdf.

BANRED (2018). Red interbancaria de Cajeros Automáticos. Recuperado de https://www.banred.fin.ec/cms54b4.html?c=1310

BBC Mundo. (2017). Tras 10 años de gobierno, además de un Ecuador dividido, ¿qué más deja Rafael Correa?. Bbc.com. Obtenido de: https://www.bbc.com/mundo/noticias-america-latina-38980926.

Buchmann, J. (2013). Introduction to cryptography. Springer Science & Business Media.

Cambridge University Press. (2018). Cambridge Academic Content Dictionary. Dictionary.cambridge.org. Obtenido de: https://dictionary.cambridge.org/es/diccionario/ingles/atm

Del Carpio Gallegos, J. (2006). Análisis del riesgo en la administración de proyectos de tecnología de información. Industrial Data, 9(1).

Diffie, W., & Hellman, M. E. (1976, June). Multiuser cryptographic techniques. In Proceedings of the June 7-10, 1976, national computer conference and exposition (pp. 109-112). ACM.).

El Comercio (2017). ¿Cómo está Ecuador en materia de Ciberseguridad?. ElComercio.com. Obtenido de https://www.elcomercio.com/guaifai/ecuador-seguridad-internet-hackeo-ciberataque.html

EMVCo. (2016). Book A: Architecture and General Requirements. Emvco.com. Obtenido de: https://www.emvco.com/wp-content/uploads/2017/05/Book_A_Architecture_and_General_Rqmts_v2_6_Final_20160422011856105.pdf

Galbraith, S. D. (2012). Mathematics of public key cryptography. Cambridge University Press

Giménez, V. M. (2011). Hacking y ciberdelito (Doctoral dissertation).

Hellman, M. E. (1979). The mathematics of public-key cryptography. Scientific American, 241(2), 146-157.

International Organization for Standardization. (2009). ISO 31000: Risk Management: Principles and Guidelines. ISO.

ISO/IEC 27001:2013. (2013). Information technology - Security techniques - Information security management systems - Requirements (second edition). Obtenido de: http://www.iso27001security.com/html/27001.html

ISO 27000.es. (2014). Sistema de Gestión de Seguridad de la Información (SGSI). Iso27000.es. Obtenido de: http://www.iso27000.es/download/doc_sgsi_all.pdf

ISO 9001:2015. (2015). Sistemas de gestión de la calidad - Auditoría Interna.

Jin, X., Hu, X., Ying, K., Du, W., Yin, H., & Peri, G. N. (2014, November). Code injection attacks on html5-based mobile apps: Characterization, detection and mitigation. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 66-77). ACM

Kahn, D. (1996). The Codebreakers: The comprehensive history of secret communication from ancient times to the internet. Simon and Schuster.

Kamlofsky, J., Abdel Masih, S., Colombo, H., Veiga, D., & Hecht, P. (2015). Ciberdefensa de infraestructuras industriales. In XVII Workshop de Investigadores en Ciencias de la Computación. Salta.

Kenan, K. (2006). Cryptography in the database: the last line of defense. Addison-Wesley.

León, V. C. (2004). El impacto de los delitos informaticos en el desempeño organizacional. Desempeño Organizacional Retos Y Enfoques Contemporáneos, 253.

Lippmann, R., Ingols, K., Scott, C., Piwowarski, K., Kratkiewicz, K., Artz, M., & Cunningham, R.

(2006). Validating and restoring defense in depth using attack graphs.

Leitch, M. (2010). ISO 31000: 2009—The new international standard on risk management. Risk Analysis: An International Journal, 30(6), 887-892.

Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. IT Professional, 3(1), 27-32.

Monsalve-Pulido, J. A., Aponte-Novoa, F. A., & Chaves-Tamayo, D. F. (2014). Information Vulnerabilities' Study and Management, for a Private Enterprise in the Boyacá Colombian Department. Facultad de Ingeniería, 23(37), 65-72.

National Institute of Standards and Technology (2008). Technical Guide to Information Security Testing and Assessment.

NFC World (2018). *Mastercard issues timeline for contactless card and POS terminal mandates*. Obtenido de: https://www.nfcworld.com/2018/02/06/356396/mastercard-issues-timeline-contactless-card-pos-terminal-mandates/

Núñez Contreras, L. (1994). Manual de paleografía. Fundamentos e historia de la escritura latina hasta el siglo VIII.

OWASP, T. (2013). Top 10–2013. The ten most critical web application security risks.

Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.

Paredes, G. (2006). Introducción a la criptografía. *Revista Digital Universitaria*, 2-17.

PCI Security Standards Council. (2018). PCI DSS Quick Reference Guide. Pcisecuritystandards.org. Obtenido de: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1540416603405

Purdy, G. (2010). ISO 31000: 2009—setting a new standard for risk management. Risk Analysis: An International Journal, 30(6), 881-886.

Shannon, C. E. (1948). A mathematical theory of communication. Bell system technical journal, 27(3), 379-423.

Smith, R. E. (1995). Sidewinder: Defense in depth using type enforcement. International Journal of Network Management, 5(4), 219-229.

Superintendencia de Bancos del Ecuador. (2014). Resolución JB-20144-3066. Sbs.gob.ec. Obtenido de: http://oidprd.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2014/resol_JB-2014-3066.pdf

Ministerio de Finanzas del Ecuador. (2014). Presupuesto general del estado - Programa anual de inversiones. Finanzas.gob.ec. Obtenido de: https://www.finanzas.gob.ec/wp-content/uploads/downloads/2014/06/PAI_PROYECTO.pdf

Triguero, J. J. O., Guerrero, M. Á. L., & del Castillo Crespo, E. C. G. (2005). Introducción a la criptografía: historia y actualidad (Vol. 50). Univ de Castilla La Mancha

Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process (SCRMP). Supply Chain Management: An International Journal, 16(6), 474-483.

Zheng, Y., & Imai, H. (1998). Compact and unforgeable key establishment over an ATM network. In INFOCOM'98. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE (Vol. 2, pp. 411-418). IEEE.

ANEXOS

Anexo 1.- Contenido de la encuesta.

ENCUESTA PARA ANÁLISIS DE CICLO DE VIDA DE LLAVES DE CIFRADO DE CAJEROS AUTOMÁTICOS PARA ENTIDADES FINANCIERAS DEL ECUADOR

Descripción: La encuesta va dirigida al personal que labora en áreas relacionadas a la informática, seguridad, operación o que tenga alguna relación en los procesos administrativos de llaves de cifrado en cajeros automáticos para entidades financieras del Ecuador.

Nombres y Apellidos:_____

Correo / número de teléfono personal / Empresa en la que trabaja (todas son opcionales):

_____

1.- ¿Cuál es el tipo de entidad financiera en la que usted trabaja?

- □ Banco
- □ Cooperativa de ahorro y crédito
- □ Servicios Transaccionales de Cobros y Pagos
- □ Red interbancaria de cajeros automáticos

2.- ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja?

- □ Ethical Hacking para cajeros automáticos
- □ Evaluación riesgo financiero: pérdidas económicas y reputación
- □ GAP Análisis PCI DSS
- □ Ninguna de las anteriores

3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos?

- □ Manuales y procedimientos
- □ Clasificación de activos de la información
- □ Compromiso de la alta dirección
- □ Personal capacitado en temas de seguridad informática

4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?

- □ Manuales y procedimientos.
- □ Clasificación de activos de la información
- □ Compromiso de la alta dirección
- □ Personal capacitado en temas de seguridad informática

5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?

- □ Manuales y procedimientos.
- □ Clasificación de activos de la información
- □ Compromiso de la alta dirección
- □ Personal capacitado en temas de seguridad informática

6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos?

- □ Manuales y procedimientos.
- □ Clasificación de activos de la información
- □ Compromiso de la alta dirección
- □ Personal capacitado en temas de seguridad informática

7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información?

- □ PCI DSS
- □ ISO 27001
- □ Estándar de cifrado OWASP
- □ Estándar de cifrado NIST
- □ Evaluación riesgo financiero: pérdidas económicas y reputación

8.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad informática?

- □ PCI DSS
- □ ISO 27001
- □ Estándar de cifrado OWASP

- □ Estándar de cifrado NIST
- □ Evaluación riesgo financiero: pérdidas económicas y reputación

9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?

- □ PCI DSS
- □ ISO 27001
- □ Estándar de cifrado OWASP
- □ Estándar de cifrado NIST
- □ Evaluación riesgo financiero: pérdidas económicas y reputación

10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?

- □ PCI DSS
- □ ISO 27001
- □ Estándar de cifrado OWASP
- □ Estándar de cifrado NIST
- □ Evaluación riesgo financiero: pérdidas económicas y reputación

11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?

- □ PCI DSS
- □ ISO 27001
- □ Evaluación riesgo financiero: pérdidas económicas y reputación

12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?

- □ Certificación internacional PCI DSS
- □ Certificación ISO 27001
- □ Cumplimiento OWASP
- □ Cumplimiento NIST

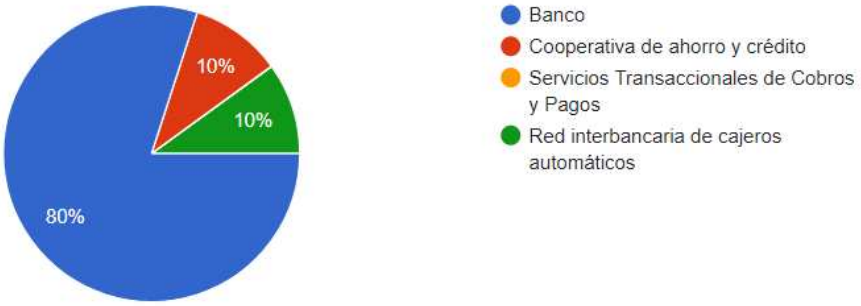
13.- ¿Qué requisitos deben cumplir el hardware y software relacionado a llaves de cifrado?

- Certificación PCI DSS
- Certificación ISO 27001
- Cumplimiento OWASP
- Cumplimiento NIST

Anexo 2.- Tabulación de resultados

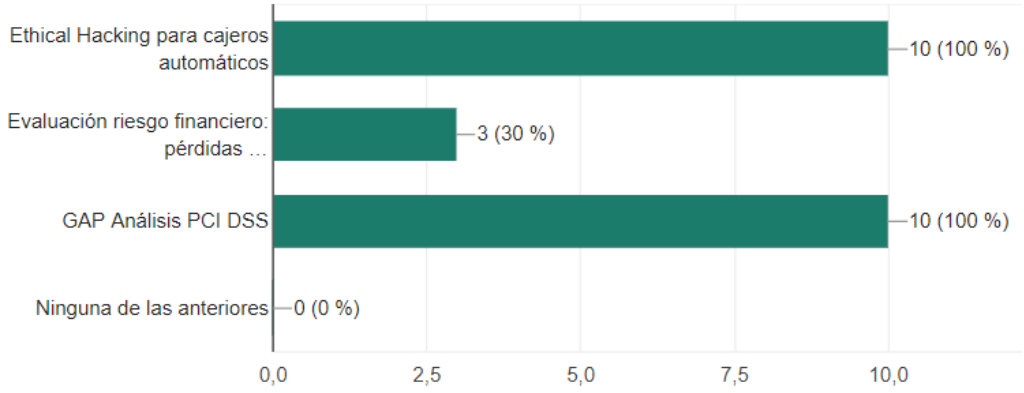
1.- ¿Cuál es el tipo de entidad financiera en la que usted trabaja?

10 respuestas



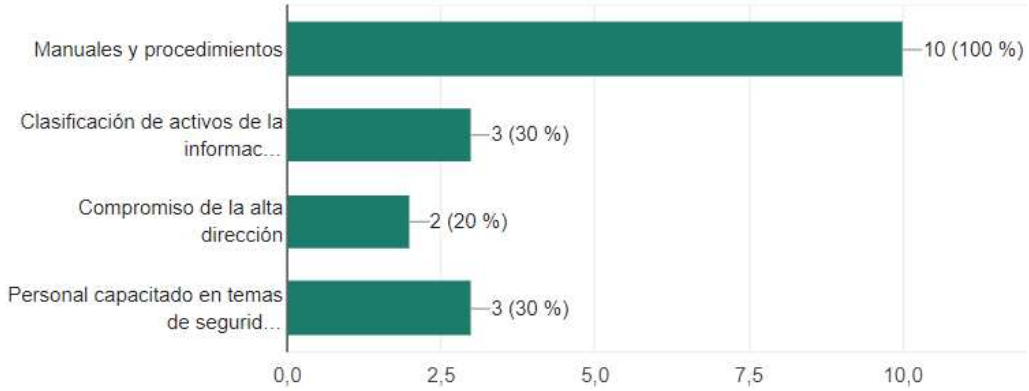
2.- ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja?

10 respuestas



3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos?

10 respuestas

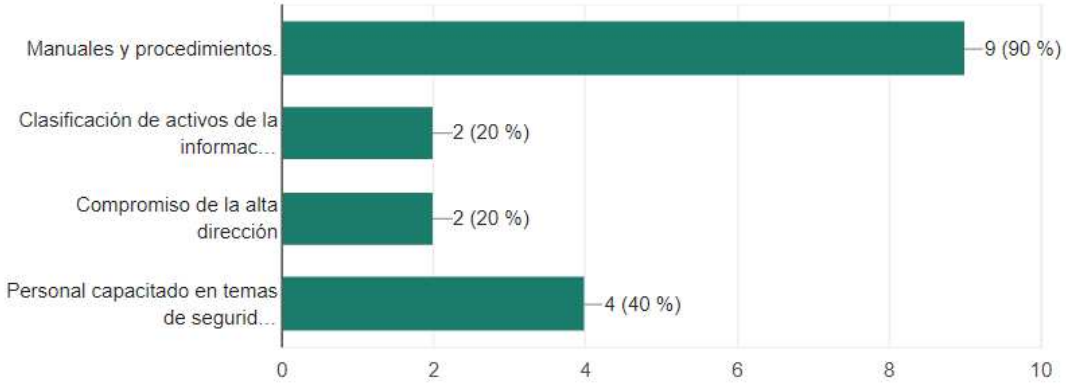


4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?

10 respuestas

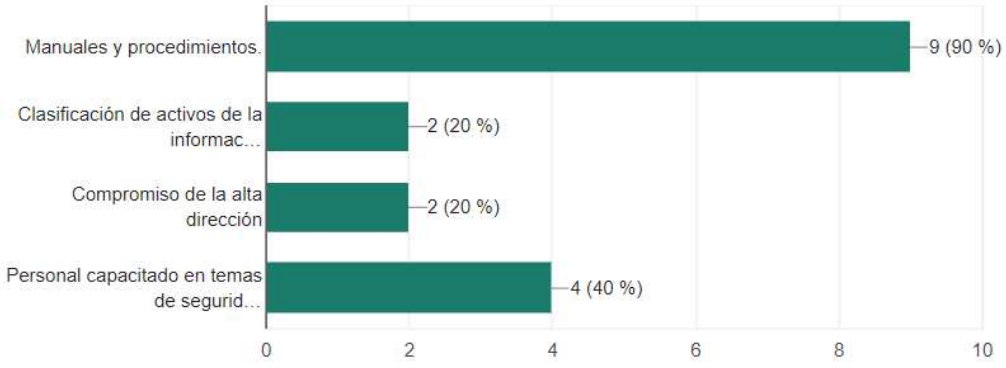
5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?

10 respuestas



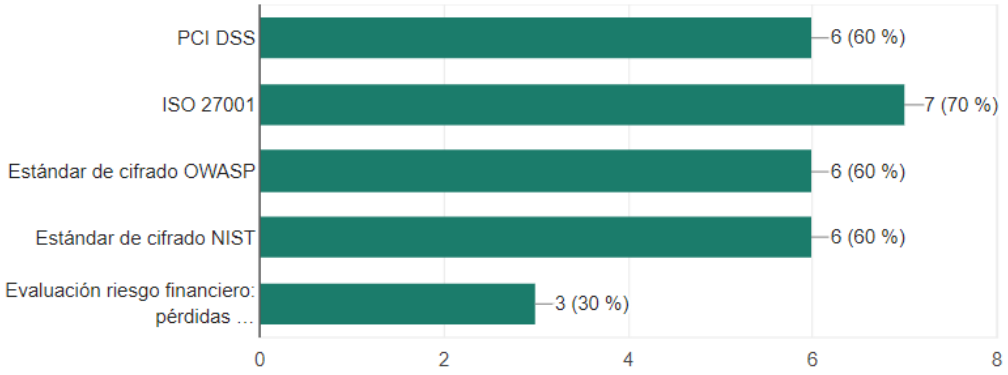
6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos?

10 respuestas



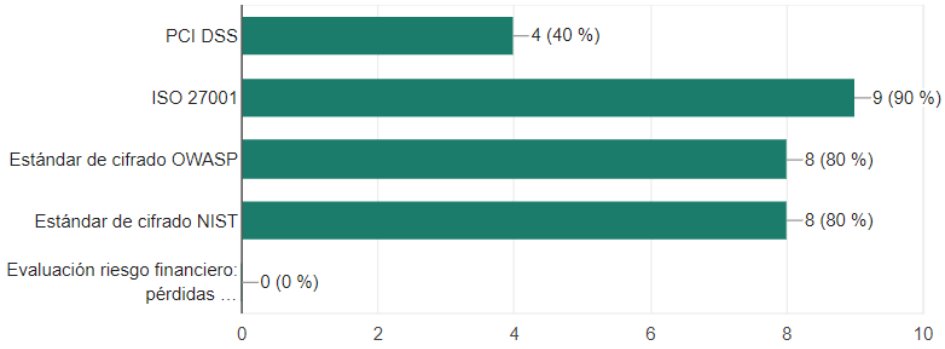
7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información?

10 respuestas



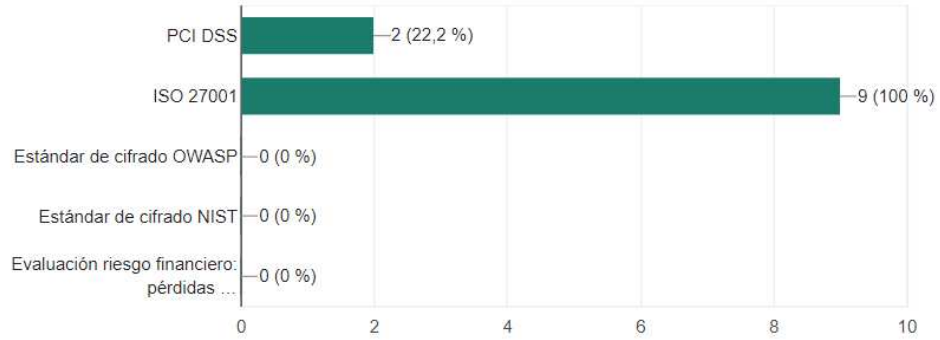
8.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad informática?

10 respuestas



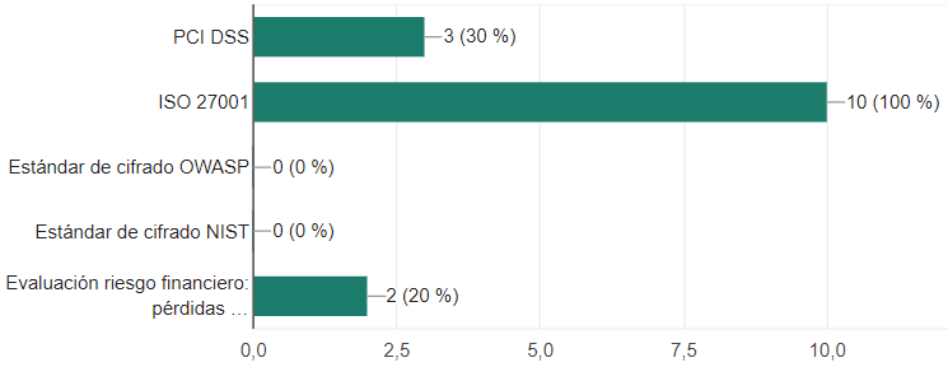
9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?

10 respuestas



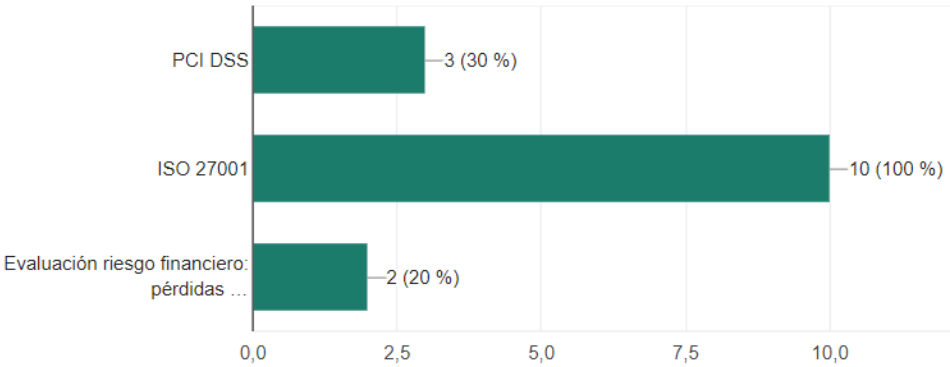
10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?

10 respuestas



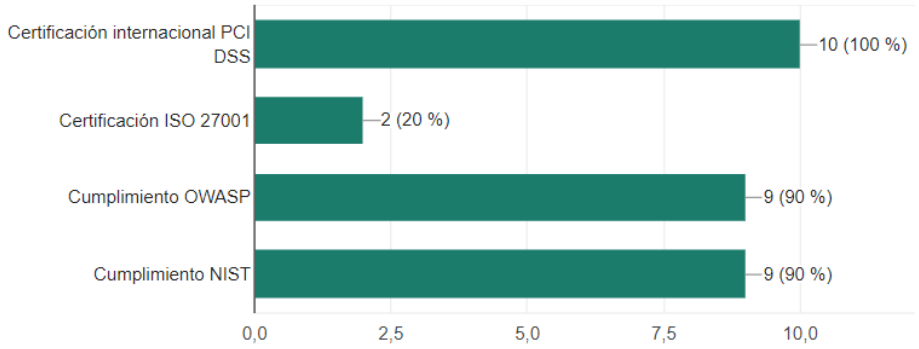
11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?

10 respuestas



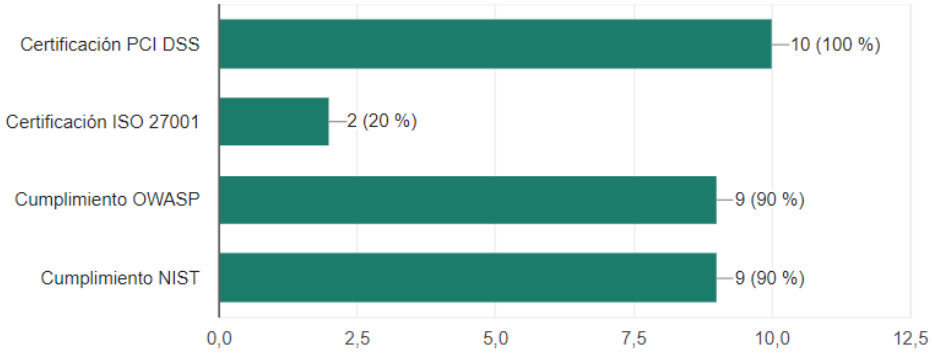
12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?

10 respuestas



13.- ¿Qué requisitos deben cumplir el hardware y software relacionado a llaves de cifrado?

10 respuestas



Anexo 3.- La encuesta es de elaboración propia, a continuación se sustenta el proceso de elaboración en base a la normativa.

Preguntas propuestas	Sustento normativo y legal	Justificación
1.- ¿Cuál es el tipo de entidad financiera en la que usted trabaja?	✓ No Aplica.	Se utiliza para clasificar el universo de los encuestados.
2 ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja?	✓ Art. 22.8, Sección VII, Título X, Capítulo V del Libro I Normas generales para la aplicación de la ley general de instituciones del sistema financiero del Ecuador. ✓ Requisito 11.3 de PCI DSS v3.2	Los artículos de las normativas recomiendan realizar auditorías informáticas de manera general, el autor, en base a buenas prácticas de auditoría, ha enfocado la recomendación al sistema en estudio.
3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos?	✓ Art. 22.5 y 22.14, Sección VII, Título X, Capítulo V del Libro I Normas generales para la aplicación de la ley general de instituciones del sistema financiero del Ecuador. ✓ Requisito 8.2 de PCI DSS v3.2	Los artículos de las normativas recomiendan gestionar el ciclo de vida de los elementos informáticos y aplicar técnicas de cifrado sobre la información crítica.
4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?	✓ Art. 22.11, Sección VII, Título X, Capítulo V del Libro I Normas generales para la aplicación de la ley general de instituciones del sistema financiero del Ecuador. ✓ Requisito 8.1.1 de PCI DSS	Los artículos de las normativas recomiendan realizar procedimientos de monitoreo de derechos, perfiles y segregación de funciones.
5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?	✓ Art. 22.5 y 22.14 Sección VII, Título X, Capítulo V del Libro I Normas generales para la aplicación de la ley general de instituciones del sistema financiero del Ecuador. ✓ Requisito 8.1.1 de PCI DSS	Los artículos de la normativa recomiendan gestionar el ciclo de vida de los elementos informáticos y aplicar técnicas de cifrado sobre la información crítica.
6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos?	✓ Art. 22.11, Sección VII, Título X, Capítulo V del Libro I Normas generales para la aplicación de la ley general de instituciones del sistema financiero del Ecuador. ✓ Requisito 8.1.2 de PCI DSS v3.2	Los artículos de las normativas recomiendan realizar procedimientos de monitoreo de actualización de derechos, perfiles y que reduzcan el riesgo de fraude.
7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información?	✓ Art. 21.3, Sección VII, Título X, Capítulo V del Libro I Normas generales para la aplicación de la ley general de instituciones del sistema financiero del Ecuador. ✓ Requisito 12.6 de PCI DSS v3.2	Los artículos de las normativas recomiendan realizar procesos de capacitación a todo el personal involucrado.
8.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad informática?	✓ Art. 21.3, Sección VII, Título X, Capítulo V del Libro I Normas generales para la aplicación de la ley general de instituciones del sistema financiero del Ecuador. ✓ Requisito 12.6 de PCI DSS v3.2	Los artículos de las normativas recomiendan realizar procesos de capacitación a todo el personal involucrado.

9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?	✓ Art. 21.3, Sección VII, Título X, Capítulo V del Libro I Normas generales para la aplicación de la ley general de instituciones del sistema financiero del Ecuador. ✓ Requisito 12.6 de PCI DSS v3.2	Los artículos de las normativas recomiendan realizar procesos de capacitación a todo el personal involucrado.
10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?	✓ Art. 21.3, Sección VII, Título X, Capítulo V del Libro I Normas generales para la aplicación de la ley general de instituciones del sistema financiero del Ecuador. ✓ Requisito 12.6 de PCI DSS v3.2	Los artículos de las normativas recomiendan realizar procesos de capacitación a todo el personal involucrado.
11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?	✓ Art. 21.3, Sección VII, Título X, Capítulo V del Libro I Normas generales para la aplicación de la ley general de instituciones del sistema financiero del Ecuador. ✓ Requisito 12.6 de PCI DSS v3.2	Los artículos de las normativas recomiendan realizar procesos de capacitación a todo el personal involucrado.
12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?	✓ A criterio del autor.	La normativa de la Junta Bancaria y la norma internacional PCI DSS recomiendan cumplir con normas internacionales, sin embargo no exigen que las entidades financieras tengan certificaciones PCI DSS, ó ISO 27001, ni cumplimiento OWASP ó cumplimiento NIST, sin embargo el autor en base a su experiencia sugiere que certificar los procesos mejorará la seguridad y reputación de las entidades financieras.
13.- ¿Qué requisitos deben cumplir el hardware ó software relacionado a llaves de cifrado?	✓ A criterio del autor.	La normativa de la Junta Bancaria y la norma internacional PCI DSS recomiendan cumplir con normas internacionales, sin embargo no exigen que las entidades financieras tengan certificaciones PCI DSS, ó ISO 27001, ni cumplimiento OWASP ó cumplimiento NIST, sin embargo el autor en base a su experiencia sugiere que certificar los procesos mejorará la seguridad y reputación de las entidades financieras

Anexo 4.- Respuestas individuales de la encuesta

ENCUESTA PARA ANÁLISIS DE CICLO DE VIDA DE CRIPTOGRAFÍA EN CAJEROS AUTOMÁTICOS PARA ENTIDADES FINANCIERAS DEL ECUADOR

La encuesta va dirigida al personal que labora en áreas relacionadas a la informática, seguridad, operación o que tenga alguna relación en los procesos administrativos de llaves de cifrado en cajeros automáticos para entidades financieras del Ecuador.

Nombres y Apellidos *

Código del encuestado: EN-01

Correo / número de teléfono personal / Empresa en la que trabaja (todas son opcionales)

Confidencial.

1.- ¿Cuál es el tipo de entidad financiera en la que usted trabaja? *

- (●) Banco
- ( ) Cooperativa de ahorro y crédito
- ( ) Servicios Transaccionales de Cobros y Pagos
- ( ) Red interbancaria de cajeros automáticos

2.- ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja? *

- [x] Ethical Hacking para cajeros automáticos
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación
- [x] GAP Análisis PCI DSS
- [ ] Ninguna de las anteriores

3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [x] Personal capacitado en temas de seguridad informática

4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?

- [ ] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [x] Personal capacitado en temas de seguridad informática

5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?

- [ ] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [x] Personal capacitado en temas de seguridad informática

6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos? *

- [ ] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [x] Personal capacitado en temas de seguridad informática

7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información? *

- [ ] PCI DSS
- [ ] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [x] Evaluación riesgo financiero: pérdidas económicas y reputación

8.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad informática?

- [ ] PCI DSS
- [x] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?

- [x] Certificación internacional PCI DSS
- [ ] Certificación ISO 27001
- [ ] Cumplimiento OWASP
- [ ] Cumplimiento NIST

13.- ¿Qué requisitos deben cumplir el hardware y software relacionado a llaves de cifrado?

- [x] Certificación PCI DSS
- [ ] Certificación ISO 27001
- [ ] Cumplimiento OWASP
- [ ] Cumplimiento NIST

ENCUESTA PARA ANÁLISIS DE CICLO DE VIDA DE CRIPTOGRAFÍA EN CAJEROS AUTOMÁTICOS PARA ENTIDADES FINANCIERAS DEL ECUADOR

La encuesta va dirigida al personal que labora en áreas relacionadas a la informática, seguridad, operación o que tenga alguna relación en los procesos administrativos de llaves de cifrado en cajeros automáticos para entidades financieras del Ecuador.

Nombres y Apellidos *

Código del encuestado: EN-02

Correo / número de teléfono personal / Empresa en la que trabaja (todas son opcionales)

Confidencial.

1.- ¿Cuál es el tipo de entidad financiera en la que usted trabaja? *

- (●) Banco
- ( ) Cooperativa de ahorro y crédito
- ( ) Servicios Transaccionales de Cobros y Pagos
- ( ) Red interbancaria de cajeros automáticos

2.- ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja? *

- [x] Ethical Hacking para cajeros automáticos
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación
- [x] GAP Análisis PCI DSS
- [ ] Ninguna de las anteriores

https://docs.google.com/forms/d/1SlZmi-dDEXHHyNaskuiibnS2TvibdhHk7Bm8YW09Vns/edit#response=ACYDBNhYFkqrejMOhH13GqLTeaORD... 1/5

3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información? *

- [ ] PCI DSS
- [x] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

8.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad informática?

- [ ] PCI DSS
- [x] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?

- [x] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?

- [x] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?

- [x] PCI DSS
- [x] ISO 27001
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?

- [x] Certificación internacional PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

13.- ¿Qué requisitos deben cumplir el hardware y software relacionado a llaves de cifrado?

- [x] Certificación PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

ENCUESTA PARA ANÁLISIS DE CICLO DE VIDA DE CRIPTOGRAFÍA EN CAJEROS AUTOMÁTICOS PARA ENTIDADES FINANCIERAS DEL ECUADOR

La encuesta va dirigida al personal que labora en áreas relacionadas a la informática, seguridad, operación o que tenga alguna relación en los procesos administrativos de llaves de cifrado en cajeros automáticos para entidades financieras del Ecuador.

Nombres y Apellidos *

Código del encuestado: EN-03

Correo / número de teléfono personal / Empresa en la que trabaja (todas son opcionales)

Confidencial.

1.- ¿Cuál es el tipo de entidad financiera en la que usted trabaja? *

- (●) Banco
- ( ) Cooperativa de ahorro y crédito
- ( ) Servicios Transaccionales de Cobros y Pagos
- ( ) Red interbancaria de cajeros automáticos

2.- ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja? *

- [x] Ethical Hacking para cajeros automáticos
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación
- [x] GAP Análisis PCI DSS
- [ ] Ninguna de las anteriores

3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información? *

- [ ] PCI DSS
- [x] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

8.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad informática?

- [ ] PCI DSS
- [x] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?

- [x] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?

- [x] Certificación internacional PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

13.- ¿Qué requisitos deben cumplir el hardware y software relacionado a llaves de cifrado?

- [x] Certificación PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

ENCUESTA PARA ANÁLISIS DE CICLO DE VIDA DE CRIPTOGRAFÍA EN CAJEROS AUTOMÁTICOS PARA ENTIDADES FINANCIERAS DEL ECUADOR

La encuesta va dirigida al personal que labora en áreas relacionadas a la informática, seguridad, operación o que tenga alguna relación en los procesos administrativos de llaves de cifrado en cajeros automáticos para entidades financieras del Ecuador.

Nombres y Apellidos *

Código del encuestado: EN-04

Correo / número de teléfono personal / Empresa en la que trabaja (todas son opcionales)

Confidencial.

1.- ¿Cuál es el tipo de entidad financiera en la que usted trabaja? *

- (●) Banco
- ( ) Cooperativa de ahorro y crédito
- ( ) Servicios Transaccionales de Cobros y Pagos
- ( ) Red interbancaria de cajeros automáticos

2.- ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja? *

- [x] Ethical Hacking para cajeros automáticos
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación
- [x] GAP Análisis PCI DSS
- [ ] Ninguna de las anteriores

3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información? *

- [x] PCI DSS
- [ ] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

8.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad informática?

- [ ] PCI DSS
- [x] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?

- [x] Certificación internacional PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

13.- ¿Qué requisitos deben cumplir el hardware y software relacionado a llaves de cifrado?

- [x] Certificación PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

ENCUESTA PARA ANÁLISIS DE CICLO DE VIDA DE CRIPTOGRAFÍA EN CAJEROS AUTOMÁTICOS PARA ENTIDADES FINANCIERAS DEL ECUADOR

La encuesta va dirigida al personal que labora en áreas relacionadas a la informática, seguridad, operación o que tenga alguna relación en los procesos administrativos de llaves de cifrado en cajeros automáticos para entidades financieras del Ecuador.

Nombres y Apellidos *

Código del encuestado: EN-05

Correo / número de teléfono personal / Empresa en la que trabaja (todas son opcionales)

Confidencial.

1.- ¿Cuál es el tipo de entidad financiera en la que usted trabaja? *

- (●) Banco
- ( ) Cooperativa de ahorro y crédito
- ( ) Servicios Transaccionales de Cobros y Pagos
- ( ) Red interbancaria de cajeros automáticos

2.- ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja? *

- [x] Ethical Hacking para cajeros automáticos
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación
- [x] GAP Análisis PCI DSS
- [ ] Ninguna de las anteriores

3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información? *

- [x] PCI DSS
- [ ] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

8.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad informática?

- [x] PCI DSS
- [ ] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?

- [ ] PCI DSS
- [ ] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?

- [x] Certificación internacional PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

13.- ¿Qué requisitos deben cumplir el hardware y software relacionado a llaves de cifrado?

- [x] Certificación PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

ENCUESTA PARA ANÁLISIS DE CICLO DE VIDA DE CRIPTOGRAFÍA EN CAJEROS AUTOMÁTICOS PARA ENTIDADES FINANCIERAS DEL ECUADOR

La encuesta va dirigida al personal que labora en áreas relacionadas a la informática, seguridad, operación o que tenga alguna relación en los procesos administrativos de llaves de cifrado en cajeros automáticos para entidades financieras del Ecuador.

Nombres y Apellidos *

Código del encuestado: EN-06

Correo / número de teléfono personal / Empresa en la que trabaja (todas son opcionales)

Confidencial.

1.- ¿Cuál es el tipo de entidad financiera en la que usted trabaja? *

- (●) Banco
- ( ) Cooperativa de ahorro y crédito
- ( ) Servicios Transaccionales de Cobros y Pagos
- ( ) Red interbancaria de cajeros automáticos

2.- ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja? *

- [x] Ethical Hacking para cajeros automáticos
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación
- [x] GAP Análisis PCI DSS
- [ ] Ninguna de las anteriores

3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información? *

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

8.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad informática?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?

- [x] Certificación internacional PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

13.- ¿Qué requisitos deben cumplir el hardware y software relacionado a llaves de cifrado?

- [x] Certificación PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

ENCUESTA PARA ANÁLISIS DE CICLO DE VIDA DE CRIPTOGRAFÍA EN CAJEROS AUTOMÁTICOS PARA ENTIDADES FINANCIERAS DEL ECUADOR

La encuesta va dirigida al personal que labora en áreas relacionadas a la informática, seguridad, operación o que tenga alguna relación en los procesos administrativos de llaves de cifrado en cajeros automáticos para entidades financieras del Ecuador.

Nombres y Apellidos *

Código del encuestado: EN-07

Correo / número de teléfono personal / Empresa en la que trabaja (todas son opcionales)

Confidencial.

1.- ¿Cuál es el tipo de entidad financiera en la que usted trabaja? *

- (●) Banco
- ( ) Cooperativa de ahorro y crédito
- ( ) Servicios Transaccionales de Cobros y Pagos
- ( ) Red interbancaria de cajeros automáticos

2.- ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja? *

- [x] Ethical Hacking para cajeros automáticos
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación
- [x] GAP Análisis PCI DSS
- [ ] Ninguna de las anteriores

3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos
- [x] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información? *

- [x] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

8.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad informática?

- [x] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?

- [x] Certificación internacional PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

13.- ¿Qué requisitos deben cumplir el hardware y software relacionado a llaves de cifrado?

- [x] Certificación PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

ENCUESTA PARA ANÁLISIS DE CICLO DE VIDA DE CRIPTOGRAFÍA EN CAJEROS AUTOMÁTICOS PARA ENTIDADES FINANCIERAS DEL ECUADOR

La encuesta va dirigida al personal que labora en áreas relacionadas a la informática, seguridad, operación o que tenga alguna relación en los procesos administrativos de llaves de cifrado en cajeros automáticos para entidades financieras del Ecuador.

Nombres y Apellidos *

Código del encuestado: EN-08

Correo / número de teléfono personal / Empresa en la que trabaja (todas son opcionales)

Confidencial.

1.- ¿Cuál es el tipo de entidad financiera en la que usted trabaja? *

- (●) Banco
- ( ) Cooperativa de ahorro y crédito
- ( ) Servicios Transaccionales de Cobros y Pagos
- ( ) Red interbancaria de cajeros automáticos

2.- ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja? *

- [x] Ethical Hacking para cajeros automáticos
- [x] Evaluación riesgo financiero: pérdidas económicas y reputación
- [x] GAP Análisis PCI DSS
- [ ] Ninguna de las anteriores

https://docs.google.com/forms/d/1SlZmi-dDEXHHyNaskuiibnS2TvibdhHk7Bm8YW09Vns/edit#response=ACYDBNjvc7JnFE4yodomFvrt8XU8oBI... 1/5

3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos
- [x] Clasificación de activos de la información
- [x] Compromiso de la alta dirección
- [x] Personal capacitado en temas de seguridad informática

4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [x] Clasificación de activos de la información
- [x] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [x] Clasificación de activos de la información
- [x] Compromiso de la alta dirección
- [x] Personal capacitado en temas de seguridad informática

6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos.
- [x] Clasificación de activos de la información
- [x] Compromiso de la alta dirección
- [x] Personal capacitado en temas de seguridad informática

7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información? *

- [x] PCI DSS
- [x] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [x] Evaluación riesgo financiero: pérdidas económicas y reputación

8.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad informática?

- [x] PCI DSS
- [x] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?

- [x] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [x] Evaluación riesgo financiero: pérdidas económicas y reputación

11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?

- [x] PCI DSS
- [x] ISO 27001
- [x] Evaluación riesgo financiero: pérdidas económicas y reputación

12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?

- [x] Certificación internacional PCI DSS
- [x] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

13.- ¿Qué requisitos deben cumplir el hardware y software relacionado a llaves de cifrado?

- [x] Certificación PCI DSS
- [x] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

ENCUESTA PARA ANÁLISIS DE CICLO DE VIDA DE CRIPTOGRAFÍA EN CAJEROS AUTOMÁTICOS PARA ENTIDADES FINANCIERAS DEL ECUADOR

La encuesta va dirigida al personal que labora en áreas relacionadas a la informática, seguridad, operación o que tenga alguna relación en los procesos administrativos de llaves de cifrado en cajeros automáticos para entidades financieras del Ecuador.

Nombres y Apellidos *

Código del encuestado: EN-09

Correo / número de teléfono personal / Empresa en la que trabaja (todas son opcionales)

Confidencial.

1.- ¿Cuál es el tipo de entidad financiera en la que usted trabaja? *

- ○ Banco
- ○ Cooperativa de ahorro y crédito
- ○ Servicios Transaccionales de Cobros y Pagos
- ◉ Red interbancaria de cajeros automáticos

2.- ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja? *

- ☑ Ethical Hacking para cajeros automáticos
- ☑ Evaluación riesgo financiero: pérdidas económicas y reputación
- ☑ GAP Análisis PCI DSS
- ☐ Ninguna de las anteriores

https://docs.google.com/forms/d/1SIZmi-dDEXHHyNaskuiibnS2TvibdhHk7Bm8YW09Vns/edit#response=ACYDBNjk2oC8Bw6-Le3dxUkz6JXp4R... 1/5

3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos
- [x] Clasificación de activos de la información
- [x] Compromiso de la alta dirección
- [x] Personal capacitado en temas de seguridad informática

4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [x] Clasificación de activos de la información
- [x] Compromiso de la alta dirección
- [x] Personal capacitado en temas de seguridad informática

5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [x] Clasificación de activos de la información
- [x] Compromiso de la alta dirección
- [x] Personal capacitado en temas de seguridad informática

6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos.
- [x] Clasificación de activos de la información
- [x] Compromiso de la alta dirección
- [x] Personal capacitado en temas de seguridad informática

7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información? *

- [x] PCI DSS
- [x] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [x] Evaluación riesgo financiero: pérdidas económicas y reputación

8.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad informática?

- [x] PCI DSS
- [x] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?

- [x] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [x] Evaluación riesgo financiero: pérdidas económicas y reputación

11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?

- [x] PCI DSS
- [x] ISO 27001
- [x] Evaluación riesgo financiero: pérdidas económicas y reputación

12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?

- [x] Certificación internacional PCI DSS
- [x] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

13.- ¿Qué requisitos deben cumplir el hardware y software relacionado a llaves de cifrado?

- [x] Certificación PCI DSS
- [x] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

ENCUESTA PARA ANÁLISIS DE CICLO DE VIDA DE CRIPTOGRAFÍA EN CAJEROS AUTOMÁTICOS PARA ENTIDADES FINANCIERAS DEL ECUADOR

La encuesta va dirigida al personal que labora en áreas relacionadas a la informática, seguridad, operación o que tenga alguna relación en los procesos administrativos de llaves de cifrado en cajeros automáticos para entidades financieras del Ecuador.

Nombres y Apellidos *

Código del encuestado: EN-10

Correo / número de teléfono personal / Empresa en la que trabaja (todas son opcionales)

Confidencial.

1.- ¿Cuál es el tipo de entidad financiera en la que usted trabaja? *

- ○ Banco
- ◉ Cooperativa de ahorro y crédito
- ○ Servicios Transaccionales de Cobros y Pagos
- ○ Red interbancaria de cajeros automáticos

2.- ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja? *

- ☑ Ethical Hacking para cajeros automáticos
- ☑ Evaluación riesgo financiero: pérdidas económicas y reputación
- ☑ GAP Análisis PCI DSS
- ☐ Ninguna de las anteriores

3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [ ] Personal capacitado en temas de seguridad informática

5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [x] Personal capacitado en temas de seguridad informática

6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos? *

- [x] Manuales y procedimientos.
- [ ] Clasificación de activos de la información
- [ ] Compromiso de la alta dirección
- [x] Personal capacitado en temas de seguridad informática

7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información? *

- [x] PCI DSS
- [x] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

8.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad informática?

- [ ] PCI DSS
- [x] ISO 27001
- [x] Estándar de cifrado OWASP
- [x] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Estándar de cifrado OWASP
- [ ] Estándar de cifrado NIST
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?

- [ ] PCI DSS
- [x] ISO 27001
- [ ] Evaluación riesgo financiero: pérdidas económicas y reputación

12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?

- [x] Certificación internacional PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

13.- ¿Qué requisitos deben cumplir el hardware y software relacionado a llaves de cifrado?

- [x] Certificación PCI DSS
- [ ] Certificación ISO 27001
- [x] Cumplimiento OWASP
- [x] Cumplimiento NIST

Anexo 5.- Identificación y valoración del riesgo.

Ítem	Preguntas	Causa	Evento/Riesgo	Efecto	Probabilidad	Impacto	Valor de Riesgo
R1	**2.- ¿Qué tipo de auditorías para cajeros automáticos ha realizado la entidad financiera en la que usted trabaja?**	No se ha determinado las pérdidas económicas y niveles de reputación originadas por la pérdida de confidencialidad de las llaves de cifrado	Dificultad para determinar las pérdidas económicas y niveles de reputación originadas por la pérdida de confidencialidad de las llaves de cifrado	Pérdidas económicas y disminución de reputación originadas por la pérdida de confidencialidad de las llaves de cifrado	2	4	8
R2	**3.- ¿Qué controles han sido implementados en el proceso de ADMINISTRACIÓN de llaves de cifrado para cajeros automáticos?**	Las entidades no han segregado todos los procesos de administración de llaves de cifrado porque no cuenta con recursos económicos y personal suficiente.	El proceso de administración de llaves de cifrado carece de procesos segregados y formales.	Amenaza sobre la confidencialidad, integridad y disponibilidad de llaves de cifrado de cajeros automáticos	2	4	8
R3	**4.- ¿Qué controles han sido implementados en el proceso de ASIGNACIÓN DE CUSTODIO de llaves de cifrado para cajeros automáticos?**	Las entidades no han segregado todos los procesos de asignación de custodio de llaves de cifrado porque no cuenta con recursos económicos y personal	El proceso de asignación de custodio de llaves de cifrado carece de procesos segregados y formales	Amenaza sobre la confidencialidad, integridad y disponibilidad de llaves de cifrado de cajeros automáticos	2	3	6

		suficiente.					
R4	**5.- ¿Qué controles han sido implementados en el proceso de REGISTRO de llaves de cifrado para cajeros automáticos?**	Las entidades no han segregado todos los procesos de registro de llaves de cifrado porque no cuenta con recursos económicos y personal suficiente.	El proceso de registro de llaves de cifrado carece de procesos segregados y formales	Amenaza sobre la confidencialidad, integridad y disponibilidad de llaves de cifrado de cajeros automáticos	2	3	6
R5	**6.- ¿Qué controles han sido implementados en el proceso de ACTUALIZACIÓN de llaves de cifrado para cajeros automáticos?**	Las entidades no han segregado todos los procesos de actualización de llaves de cifrado porque no cuenta con recursos económicos y personal suficiente.	El proceso de actualización de llaves de cifrado carece de procesos segregados y formales	Amenaza sobre la confidencialidad, integridad y disponibilidad de llaves de cifrado de cajeros automáticos	2	3	6
R6	**7.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de seguridad de la información?**	El proceso de capacitación no contempla todos los aspectos de riesgo de llaves de cajeros automáticos	Falta de capacitación al personal de seguridad de la información	Fraude y/o pérdidas económicas por errores u omisiones	3	3	9
R7	**8.- ¿Qué temas son abordados en**	El proceso de capacitación no contempla	Falta de capacitación al personal de	Fraude y/o pérdidas económicas	2	3	6

	el proceso de CAPACITACIÓN al personal de seguridad informática?	todos los aspectos de riesgo de llaves de cajeros automáticos	seguridad informática	por errores u omisiones			
R8	**9.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de operación de cajeros automáticos?**	El personal de operación trabaja todos los días con cajeros automáticos sin embargo no cuenta con la capacitación requerida	Falta de capacitación al personal de operación de cajeros automáticos	Fraude y/o pérdidas económicas por errores u omisiones	3	4	12
R9	**10.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN al personal de riesgo?**	El proceso de capacitación no contempla todos los aspectos de riesgo de llaves de cajeros automáticos	Falta de capacitación al personal de operación de riesgo	Fraude y/o pérdidas económicas por errores u omisiones	3	3	9
R10	**11.- ¿Qué temas son abordados en el proceso de CAPACITACIÓN de dirección y gerencia?**	El proceso de capacitación no contempla todos los aspectos de riesgo de llaves de cajeros automáticos	Falta de capacitación a la dirección y gerencia	Fraude y/o pérdidas económicas por errores u omisiones	2	3	6
R11	**12.- ¿Qué requisitos deben cumplir las empresas proveedoras que se encuentran relacionadas a llaves de cifrado?**	Las empresas proveedoras cumplen parcialmente con los requisitos	Falta de certificación técnica internacional de proveedores	Fraude y/o pérdidas económicas por eventual conflicto de intereses	1	2	2

R12	**13.- ¿Qué requisitos deben cumplir el hardware ó software relacionado a llaves de cifrado?**	El hardware o software cumple parcialmente con los requisitos	Falta de certificación técnica internacional de hardware	Fraude y/o pérdidas económicas por eventual conflicto de intereses	1	2	2

Anexo 6.- Plan de respuesta.

ITEM	Riesgo	Disparador	Respuesta	Acción de Respuesta	Plan de Contingencia	Quiénes el responsable
R1	No existe Unidad de detección de fraudes financieros y contables	Se recepta requerimiento de la entidad de control	Transferir	Asignar responsables para este proceso de manera formal	Establecer responsables de manera formal, separando funciones y evitando conflicto de intereses	Junta Directiva
R2	No existe Unidad de Seguridad de la Información	Se recepta requerimiento de la entidad de control	Transferir	Asignar responsables para este proceso de manera formal	Actualizar procedimientos y establecer responsables de manera formal, separando funciones y evitando conflicto de intereses.	Junta Directiva, Gerencia
R3	No existe Unidad de Seguridad de la Información	Se recepta requerimiento de la entidad de control	Transferir	Asignar responsables para este proceso de manera formal	Actualizar procedimientos y establecer responsables de manera formal, separando funciones y evitando conflicto de intereses.	Junta Directiva, Gerencia
R4	No existe Unidad de Seguridad de la Información	Se recepta requerimiento de la entidad de control	Transferir	Asignar responsables para este proceso de manera formal	Actualizar procedimientos y establecer responsables de manera formal, separando funciones y evitando conflicto de intereses.	Junta Directiva, Gerencia
R5	No existe Unidad de Seguridad de la Información	Se recepta requerimiento de la entidad de control	Transferir	Asignar responsables para este proceso de manera formal	Actualizar procedimientos y establecer responsables de manera formal, separando funciones y evitando conflicto de intereses.	Junta Directiva, Gerencia

R6	Falta de capacitación al personal de seguridad de la información	Se recepta requerimiento del área responsable	Mitigar	Actualizar el proceso de capacitación al personal de seguridad de la información	Agregar temas de PCI DSS y ethical hacking al proceso de capacitación de seguridad de la información	Riesgo Operativo
R7	Falta de capacitación al personal de seguridad informática	Se recepta requerimiento del área responsable	Mitigar	Actualizar el proceso de capacitación al personal de seguridad informática	Agregar temas de PCI DSS y ethical hacking al proceso de capacitación de seguridad de la información	Seguridad de la información
R8	Falta de capacitación al personal de operación de cajeros automáticos	Se recepta requerimiento del área responsable	Mitigar	Actualizar el proceso de capacitación al personal de operación de cajeros automáticos	Agregar temas de PCI DSS y seguridad informática básica al proceso de capacitación de seguridad de la información	Seguridad de la información
R9	Falta de capacitación al personal de operación de riesgo	Se recepta requerimiento del área responsable	Mitigar	Actualizar el proceso de capacitación al personal de riesgo	Agregar temas de PCI DSS y seguridad informática básica al proceso de capacitación de seguridad de la información	Seguridad de la información
R10	Falta de capacitación a la dirección y gerencia	Se recepta requerimiento del área responsable	Mitigar	Actualizar el proceso de capacitación de dirección y gerencia	Agregar temas de PCI DSS y seguridad informática básica al proceso de capacitación de seguridad de la información	Dirección, Gerencia
R11	Falta de certificación técnica internacional de proveedores	Se recepta requerimiento de entidad de control internacional	Aceptar	Estar informado constantemente de nuevas disposiciones que puedan darse.	Revisar las nuevas directrices y preparar un listado de acciones para cumplir con la normativa.	Riesgo Operativo
R12	Falta de certificación técnica	Se recepta requerimiento de entidad de	Aceptar	Estar informado constantemen	Revisar las nuevas directrices y preparar un listado de	Riesgo Operativo

	internacional de hardware	control internacional		te de nuevas disposiciones que puedan darse.	acciones para cumplir con la normativa.	