UNIVERSIDAD ANDRÉS BELLO

FACULTAD DE INGENIERÍA

ESCUELA DE INFORMÁTICA

PROPUESTA DE METODOLOGÍA DE DESARROLLO SEGURO DE SOFTWARE

Tesis de pregrado para optar al título de Ingeniero Civil Informático

Autor:

Benjamín Andrés Piña Gargiullo

Profesor Guía:

David Alfredo Ruete Zuñiga

SANTIAGO – CHILE

OCTUBRE, 2019

Índice general

Índice de Figuras

Índice de Tablas

CAPITULO I – PLANTEAMIENTO PROBLEMÁTICA

1.1 Introducción

En la actualidad, la red conocida como Internet se ha masificado considerablemente. Según un informe de la Subsecretaría de Telecomunicaciones correspondiente al cierre del año 2018 (Subsecretaría de Telecomunicaciones, 2019), indica que la conexión a Internet ya sea en redes fijas o móviles, han alcanzado los 21,4 millones de acceso, teniendo así un crecimiento interanual de un 10.2%, 2 millones más que en el año 2017, como resultado, existen 112,9 accesos por cada 100 habitantes en Chile, debido al aumento de dispositivos conectados por cada persona. Además, Chile se posiciona como el 8vo país con mayor acceso a internet a nivel mundial, según el ranking “The Inclusive Internet Index” realizado por The Economist (EIU Inclusive Internet Index, 2018).

Debido a lo anterior y a la posibilidad de facilitar el trabajo humano, se genera la necesidad de que todo lo que rodea a la población esté conectado, con el objetivo de que sea posible gestionar todo fácilmente mediante un móvil o algún software del tipo “Internet de las cosas ” (IoT, de sus siglas en inglés “Internet of the Things”), con el propósito de facilitar la vida a las personas con productos como televisores inteligentes, refrigeradores inteligentes e incluso ampolletas, entre otros. Sin embargo, esta misma tecnología conlleva consigo sus propios riegos, tal como el caso de la vulnerabilidad reportada en el año 2018 que afecta principalmente a los televisores inteligentes de Samsung y TCL que incluyen la plataforma Roku TV. Esta falla, permite que cualquier individuo con propósitos maliciosos sea capaz de obtener acceso a controles del televisor, como manejar el volumen, canales, reproducir contenido ofensivo, como también robar información privada que esté almacenada en estos dispositivos (Consumer Reports, 2018).

Asimismo, otras tecnologías, tales como el Big Data y el Cloud Computing, abre la posibilidad por parte de las empresas de proveer nuevos servicios, capaces de acceder tan solo con Internet y de manera más segura. Un ejemplo de esto son las Fintech o tecnología Financiera, como se conoce a las empresas que tienen como finalidad proveer distintos productos/servicios financieros innovadores, tales como, pagos o préstamos, haciendo uso de las Tecnologías de Información y Comunicación (TIC) para así acceder a estos servicios fácilmente (Lopez, 2016). Sin embargo, estas tecnologías si son manejadas de manera incorrecta pueden traer consigo problemas. En el caso del Big Data, uno de los principales problemas que trae una mala gestión de la seguridad de la información, es la pérdida de distintos tipos de datos (por ejemplo, grabaciones de cámaras de seguridad, imágenes, cuentas bancarias, información personal de diversos usuarios, etc.) y a la vez grandes cantidades de datos que son manejados (M. Rayo, 2016). En el caso del Cloud Computing, los principales problemas asociados con una mala gestión de la seguridad son la pérdida de información, integridad y/o disponibilidad de los datos. Según el artículo "*Protección de la nube (Syngress, una huella de Elsevier)"* esto se refleja en las empresas que adoptan servicios cloud de otros proveedores, debido a la poca transparencia de algunos de estos, los cuales no presentan todos sus protocolos asociados a la seguridad de la información, por lo que no se tiene plena seguridad si la información que se está procesando puede ser fácilmente vulnerada ya sea mediante ciberataques o físicamente en las instalaciones de los proveedores de este servicio (Winkler, 2016).

Por las razones ya descritas, es que estas tecnologías conllevan a tener más en consideración los riesgos asociados de estos productos o servicios que proveen las compañías, debido a que una filtración de datos sensibles puede traer riesgos financieros, operativos y afectar directamente a la integridad de los clientes, lo cual finalmente perjudica la reputación de la compañía. Por lo tanto, la seguridad de la información que maneja la empresa es muy importante para los productos y/o servicios que provee. Para esto existen normas, tales como la ISO 27001 o PCI-DSS. Estas normas, describen cómo gestionar la seguridad de la información en una organización,

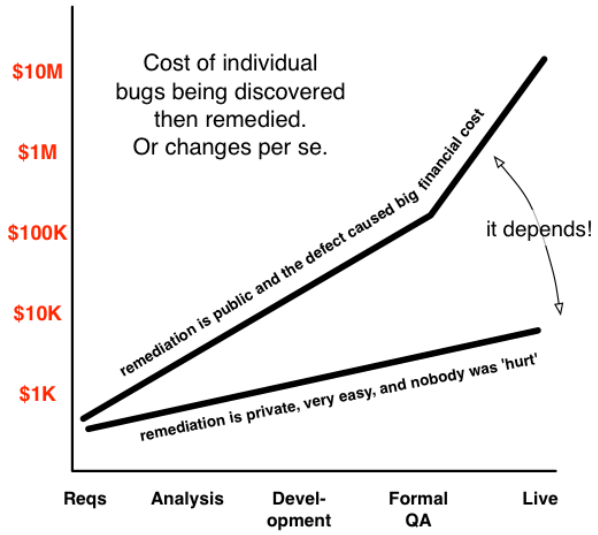
teniendo como eje central la protección de la confidencialidad, integridad y disponibilidad de la información que maneja la compañía. Para lograrlo, estas normas proponen los requisitos y controles base para proteger los datos de los clientes, con el objetivo de tener un ciclo de mejora continua en el resguardo de la información, y con ello poder identificar los GAP o Brechas de seguridad, las cuales no están en el alcance de estas normas, para posteriormente proceder a su mitigación. Sin embargo, según los datos estadísticos que provee la Organización Internacional de Estandarización (ISO), la cantidad de certificaciones en Sudamérica han crecido sustancialmente desde el año 2006, en el cual solo existían 18 certificados emitidas. En el 2010 la cifra ascendió a 117 certificaciones, y en el año 2016 la cifra aumentó a 564 certificaciones y para el año 2017 ascendió a 620 certificaciones, teniendo un crecimiento del 10% en el último periodo (2016-2017). Pero, aun así, los países sudamericanos están lejos de las cifras en las otras regiones del mundo como Norteamérica que tuvo un crecimiento del 43% entre 2016 y 2017 llegando a 2108 certificaciones, o Europa con un crecimiento del 17% llegando a 14.605 certificaciones ISO 27000/1 (GlobalSTD, 2018).

Uno de los principales problemas existentes en el incremento de desarrollo de software/aplicaciones, corresponde a un desarrollo que no contemplan los niveles básicos de seguridad de la información. Existen estudios que avalan lo mencionado, como en el informe “State of Secure Application Lifecycle Management” realizada por Creative Intellect Consulting (Firma de investigación y asesoría experta sobre entrega de software y sistemas en el mundo) (Creative Intellect Consulting (CIC), s.f.), encuesta realizada a un total de 10.000 desarrolladores de software el año 2011, el 59% aseguró que no sigue los procesos de calidad y seguridad. Además, el 26% de los encuestados aseguró que sus organizaciones tienen pocos o ningún proceso de desarrollo de software seguro (Arroyo, 2011). Un ejemplo de grandes ciberataques es el que sufrió la empresa Equifax, en la cual, un grupo de personas maliciosas accedieron a sus sistemas y robaron información, comprometiendo al menos 143 millones de datos personales de clientes, entre los cuales se obtuvieron 209.000 números de tarjetas de crédito y más de 182.000 documentos con datos personales de clientes. Según la compañía, se debió a una

vulnerabilidad en su aplicación web, la cual fue detectada en junio del 2017, y se estuvo explotando desde mayo del mismo año (Álvarez, 2017).

Por los motivos anteriormente indicados, es importante destacar la relevancia de la seguridad de la información en el desarrollo de software. Cabe mencionar que el impacto es considerablemente menor tanto a nivel monetario como de tiempo en mitigar las vulnerabilidades encontradas durante el desarrollo de un producto/software que posterior a este, debido a que una vez lanzado al mercado, influyen los clientes/usuarios que utilicen el producto, por tanto ellos también se ven afectados en caso de la explotación de una vulnerabilidad conocida o una vulnerabilidad día cero (no conocida por el grupo de trabajo), lo que afectará directamente en la imagen de la organización, como se puede visualizar en la figura 1, donde se muestra la diferencia en costos monetarios de resolver los bugs en las distintas etapas de un desarrollo de software.

Figura 1- Gráfico de costos de remediación de bugs en cada etapa de un desarrollo de software



Fuente: (Paul Hammant, 2012)

1.1.1 Marco de Trabajo

El presente trabajo se enmarca en las metodologías de desarrollo seguro actuales, tales como Secure Scrum y DevSecOps. Secure Scrum se enfoca principalmente en el desarrollo de los requisitos de seguridad de la información en un software, que según esta metodología deberían ser acordados desde un inicio con el cliente, mientras que DevSecOps se enfoca en gestionar las distintas partes de una organización (Personas, Procesos y Tecnologías) para incluir la seguridad de la información en el desarrollo de proyectos de software. Sim embargo, estas metodologías no se enfocan en dar a conocer la importancia de la seguridad de la información en el desarrollo de los productos/servicios actuales. En este contexto se desarrollará el proyecto actual, ofreciendo una metodología de desarrollo seguro, como las ya mencionadas, dando importancia a diversos temas de gestión, tales como las capacitaciones de los colaboradores correspondientes, la importancia de la concientización en seguridad de la información, como además un conjunto de buenas prácticas acordes al desarrollo de un software enmarcado en ámbitos de seguridad.

1.1.2 Motivación

Dada la necesidad de proveer diversos servicios de distintos ámbitos a través de internet, así como las consecuencias de un deficiente manejo de la seguridad de información de estos servicios, es necesario contar con un conjunto de buenas prácticas que se deberían considerar para un desarrollo seguro de software/aplicaciones en una compañía, con el objetivo de resguardar la seguridad de la información.

1.1.3 Antecedentes del problema

Actualmente, diversos problemas influyen en el déficit de desarrollo seguro de software tanto en Chile como a nivel internacional, tales como, la falta de información sobre los problemas de seguridad por parte de los colaboradores, debido principalmente a que no se ha concientizado adecuadamente sobre los riesgos asociados frente a un ciberataque o una mala gestión de la seguridad de la información, los que deberían ser abarcado según las distintas habilidades o capacidades de cada grupo de trabajadores en la organización. Sin embargo, para concientizar a los trabajadores sobre la seguridad de la información es importante mantener al grupo unido y satisfechos, ya que de lo contrario se puede generar un desinterés y por tanto desmotivación en los temas laborales. Según un estudio sobre las desmotivaciones de los colaboradores realizado por Mónica Iñaki, partner de Openmet Group, en el año 2015, uno de los principales problemas en una organización es la comunicación entre el trabajador con sus compañeros y sus superiores (Iñaki, 2015), generando así un ambiente laboral hostil, provocando desmotivación y desinterés por los temas importantes en el trabajo.

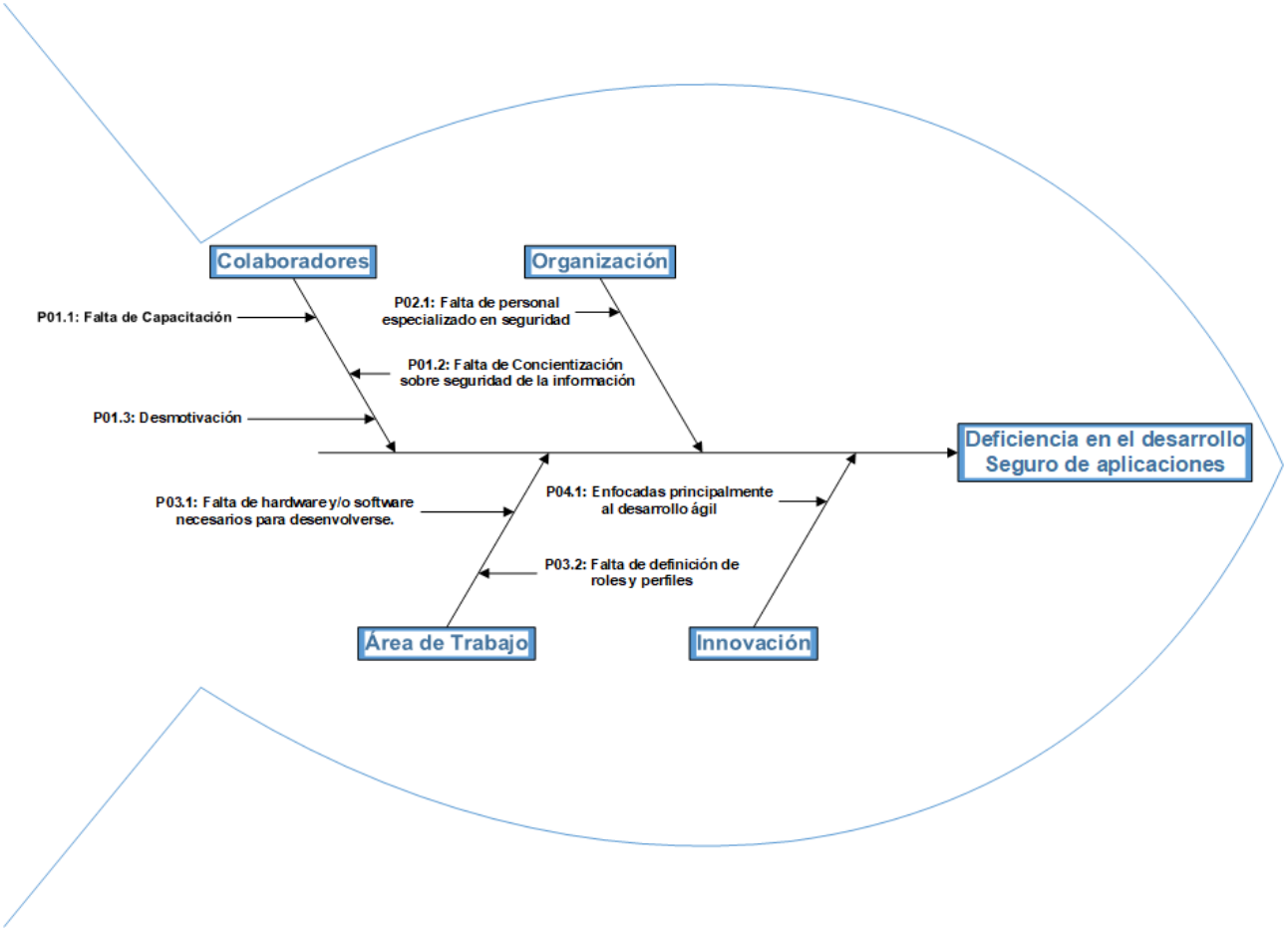
Otro problema asociado con el déficit de desarrollo seguro de software es la falta de software y/o hardware necesarios. Esto es un problema para los desarrolladores de software, debido a que se necesitan realizar diversas pruebas (funcionales y técnicas) que validen la seguridad de los códigos generados sin ningún impedimento. Asimismo, la falta de personal y/o competencias necesarias de seguridad de la información en una empresa, dificulta la determinación de los requisitos de mínimos de seguridad lógica que debe contemplar en sus desarrollos de software, por otro lado, se deben realizar pruebas técnicas o funcionales efectivas que ayuden a medir el nivel de seguridad informática. Del mismo modo, el IoT como también otras de las tecnologías actuales, entre ellas, el Big Data y Cloud Computing conllevan a que las empresas busquen innovar en productos y servicios, y lanzarlos al mercado rápidamente. Según la encuesta de “Industrial IoT Security Statistics 2017” de Tripwire (Lapena, 2017), indica que el 94% de las empresas creen que como consecuencia del IoT incremente los riesgos junto con vulnerabilidades

de sus productos y software, ya que, según expertos durante los últimos años la adopción de más soluciones asociadas al IoT (como televisores inteligentes, refrigeradores inteligentes, etc.) ha aumentado el riesgo de ataques de seguridad debido a que involucran más dispositivos conectados, además, el 51% de los encuestados afirma no estar preparado para enfrentar estas vulnerabilidades que puedan afectar a futuro. Así también, el informe “Global Markets for Security Technologies for the Internet of Thing”, realizado por bccResearch (editora de informes de investigación de los mercados de tecnología, reseñas y boletines técnicos) (bccResearch, s.f.), afirma que después del ciberataque al proveedor de DNS DynDNS, incluso las grandes empresas como Amazon, PayPal y Twitter, se han dado cuenta de la necesidad de implementar prácticas de seguridad para IoT, además, se predice que al 2020 las violaciones de seguridad asociadas al IoT podrían aumentar un 25% (Velykholova, 2017).

1.2 Identificación del problema

A partir de lo mencionado, se establece la problemática con sus respectivas causas, estas serán mencionadas en el diagrama Ishikawa correspondiente a la Figura 2.

Figura 2 – Diagrama de Ishikawa



Fuente: Elaboración Propia

1.3 Objetivos e Hipótesis

1.3.1 Objetivo General

Mejorar el desarrollo de software/aplicaciones, contemplando un marco de la seguridad de la información, mediante el diseño de una Metodología de Desarrollo de Software Seguro, con el fin de reducir los potenciales riesgos que puedan materializarse en un futuro y que no tengan impacto directo en el negocio.

1.3.2 Objetivos Específicos

Para la definición de los objetivos específicos del proyecto, se basarán en el tipo de objetivos S.M.A.R.T. Este tipo de objetivos se describen por 5 características fundamentales: Especifico, Medible, Alcanzable, Realista y En tiempo, como se podrá visualizar en la figura a continuación.

Figura 3 – Siglas objetivos SMART

Fuente: (Dana, 2017)

A continuación, se definirán los objetivos específicos del proyecto actual, para luego relacionarlos con cada una de las preguntas que debería responder un objetivo S.M.A.R.T.

O.E01: Entregar lineamientos básicos que se deben contemplar para un desarrollo seguro de software.

O.E02: Proveer información sobre la importancia de la seguridad de la información en el desarrollo de aplicaciones mediante un plan de sensibilización sobre la seguridad de la información. (Ver Anexo A2)

O.E03: Proveer un checklist de las tareas que debe contemplar un software seguro. (Ver Anexo A1)

Para el objetivo específico 1, se considera S.M.A.R.T, ya que es realizable y puede ser verificado con los indicadores obtenidos, además, se puede realizar en el tiempo en que durará la prueba de la metodología. Con respecto al O.E02, se considera un objetivo S.M.A.R.T, ya que es posible informar a los colaboradores de la importancia de la seguridad de la información en del desarrollo de software mediante un plan de sensibilización en un tiempo determinado, y este puede medirse con la creación y entrega de un plan de concientización, así como los indicadores que se obtendrán a partir de este con las evaluaciones realizadas para cada concientización, sabiendo así cuales son los temas que se deben reforzar en el equipo de trabajo. Finalmente, en el O.E03 se considera un objetivo S.M.A.R.T, ya que el checklist es realizable en un tiempo determinado además se puede medir con la entrega de este, junto con diversas métricas asociadas a la adherencia de estos controles, así como cuáles son los controles con mayor y menor adherencias (ya sea separados por categoría o por controles como tal), los que serán relevantes para sacar conclusiones sobre el desarrollo de diversos proyectos.

1.3.2 Matriz de Trazabilidad

En la tabla 1 se visualiza la trazabilidad de los problemas identificados en el Diagrama de Ishikawa, con los distintos objetivos que aportarán a la solución de estos.

Tabla 1 - Matriz de Trazabilidad

O. Específico / Problema	P01.1	P01.2	P01.3	P02.1	P02.2	P03.1	P04.1
OE01	✔	✔	✔	✔	✔	✔	✔
OE02	✔	✔	✔		✔	✔	✔
OE03	✔	✔			✔	✔	✔

Fuente: Elaboración Propia

1.3.4 Calidad de los Objetivos

Tabla 2 - Métricas de Objetivos Específicos

O. Específico	Métrica	Unidad	VAM	CEM
O.E01: Entregar lineamientos básicos que se deben contemplar para un desarrollo seguro de software.	Determina la cantidad de vulnerabilidades de carácter medio, alto o crítico presentes en un proyecto de software, el cual será basado una metodología de desarrollo seguro, mediante un Ethical hacking (EH) y/o un escáner de vulnerabilidades (VA).	#	0	$Cv \leq 3$ en promedio (basada en críticas, altas, medias)
O.E02: Proveer información sobre la importancia de la seguridad de la información en el desarrollo de aplicaciones mediante un plan de sensibilización sobre la seguridad de la información.	Cantidad de reuniones o charlas en un mes.	#	0	$Cr \geq 1$ por mes
O.E03: Proveer un checklist de las tareas que debe contemplar un software seguro.	Entregar un conjunto de buenas prácticas que al menos deben considerarse en un ciclo de desarrollo de software seguro	N.A	0	Checklist de las tareas básicas que debe cumplir un software seguro.

Fuente: Elaboración Propia

1.3.5 Hipótesis

Una metodología enmarcada en el desarrollo seguro de software no es capaz de reducir la cantidad de vulnerabilidades de carácter críticas, altas o medias, que puedan materializarse en los sistemas y/o aplicaciones desarrolladas en un futuro.

1.4 Alcances, Limitaciones y Supuestos

1.4.1 Alcances

1. Proveer un conjunto de recomendaciones al momento de desarrollar un software seguro, tales como, las capacitaciones que deberían tener los colaboradores, etc.
2. Proveer los lineamientos bases de gestión para desarrollar un software seguro.
3. Proveer recomendaciones de los diversos temas que pueden ser abordado en el plan de concientización.

1.4.2 Limitaciones al alcance

1. Se enfocará principalmente a los grupos de desarrollo de software que tiendan a la utilización de metodologías de desarrollo ágiles como Scrum o DevOps.
2. No se dará a conocer el cómo realizar las tareas asociadas al checklist, sino lo que debe hacer para aportar a la seguridad de la información del software que se está desarrollando.
3. No se entregará una herramienta para evaluar la seguridad del software, sino que solo se proveerá la conceptualización de cómo puede medirse, pero es responsabilidad del equipo de trabajo realizarlo.
4. El checklist será realizado solamente en base a la norma ISO 27001\2, PCI-DSS v3.2 y el ranking de vulnerabilidades OWASP Top 10.
5. Dada la duración para la realización del proyecto, el tiempo para realizar las pruebas en un ambiente real del proyecto no son suficientes, debido a que este debe ser probado en proyectos reales los cuales tienen, a lo menos, una duración no menor a 2 meses, por lo que se considerarán para los resultados, las vulnerabilidades encontradas en proyectos en distintas etapas de su desarrollo.

1.4.3 Supuestos

1. El grupo de trabajo ejecutará correctamente los lineamientos entregados por esta metodología.
2. La organización contemplará y velará por el cumplimiento de las tareas ofrecidas en el checklist.

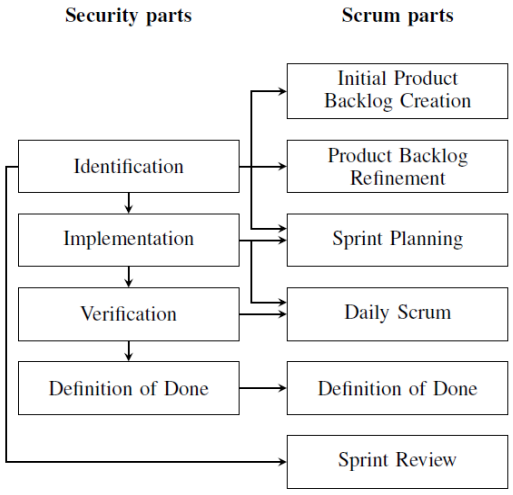
CAPÍTULO II - DISCUSIÓN Y MARCO TEÓRICO

2.1. Marco Teórico

2.1.1. Secure Scrum

Es una variante de la metodología de desarrollo ágil Scrum, el que tiene como finalidad identificar las partes de seguridad relevantes de un proyecto de software, para así tener un apropiado nivel de seguridad (se debe asegurar hasta que ya no sea rentable para un intruso encontrar y explotar una vulnerabilidad) (Pohl & Holf, 2015). Secure Scrum consta de 4 etapas principales: Identificación, Implementación, Verificación y Definición de componente realizado. Estos componentes anteriores son integrados con las etapas ya definidas en el marco de trabajo de Scrum, como se mostrará en la figura 4.

Figura 4 – Integración de Secure Scrum en Scrum tradicional



Fuente: (Pohl & Holf, 2015)

Como se visualiza en la figura 4, se tiene la integración de los procesos de seguridad en los de Scrum estándar. A continuación, se describirá cada uno de estos procesos y como se integra con las etapas ya conocidas.

Identificación de componentes

Esta etapa consiste en identificar y marcar las historias de usuarios relevantes para la seguridad. Como se vio en la figura 4, esta etapa está contenida en la creación del Product Backlog inicial, durante el Sprint Planning y el refinamiento del Sprint. En un principio el Product Owner y los miembros del equipo de trabajo, rankean las historias de usuarios de acuerdo con su valor perdido (perdida que se tiene cuando el software es vulnerado por la funcionalidad asociada a esta historia de usuario). Luego se ordenan según los riesgos de este, para finalmente documentarlos asociando las historias de usuario con “S-tags” los que describen los posibles riesgos de seguridad encontrados anteriormente.

Implementación de componentes

En Secure Scrum, al igual que en Scrum tradicional, en un sprint se implementa un subconjunto de funcionalidades, a diferencia que en el sprint backlog se debe incluir los S-tag asociados a las historias de usuario a implementar, los que se pueden dividir igualmente en un conjunto de tareas para su implementación, pero siempre asociado a la funcionalidad a la que se asignó.

Verificación de componentes y definición de hechos

Al igual que en Scrum, esta etapa consiste en la realización de las pruebas pertinentes a las tareas realizadas de los S-tag, para así comprobar el cumplimiento de

los criterios de calidad planteados en la definición de hechos, además de que se mantenga la asociación entre las tareas de los S-tag y las funcionalidades a las que se asignaron. Cabe destacar que para los distintos procesos asociados a Secure Scrum, es posible incluir recursos externos, por ejemplo, consultores de seguridad, con la finalidad de mejorar el conocimiento sobre seguridad al equipo de Scrum, resolver distintos desafíos para cubrir los posibles riesgos de vulnerabilidades, además de proveer una visión externa, para así identificar las formas de vulnerar nuestro propio sistema.

Para el caso de este proyecto, Secure Scrum se utilizará para extraer ideas de la metodología, tal como, la gestión de los requisitos de seguridad asociado a las historias de usuario, para integrarlas en la metodología a desarrollar y así obtener un mejor resultado.

2.1.2. DevSecOps

Es una metodología de desarrollo de software seguro, enfocada principalmente en la gestión de los recursos, la que se caracteriza por ayudar a identificar problemas de seguridad al comienzo del proceso de desarrollo y no después de lanzado el producto, con la finalidad de reducir costos y aumentar la velocidad de recuperación frente a un incidente de seguridad, entre otros (Raynaud, 2017). DevSecOps plantea el incluir la seguridad de la información en las metodologías ágiles tradicionales. Para esto, se basa en buenas prácticas asociado a 3 conceptos: personas, procesos y tecnología, los que serán descrito a continuación.

Personas

Para DevSecOps el factor humano siempre será la gran debilidad en la seguridad de un software. Además, actualmente la utilización de metodologías agiles ayuda a lanzar productos rápidamente, pero, a menudo a costa de descuidar la seguridad de estos. Por esta razón, plantea que para que las seguridades de estas aplicaciones sean efectivos, se debe incluir personal de seguridad lo más temprano posible en el ciclo de vida del software. Para esto, la metodología considera como elemento clave a los Campeones de Seguridad en el grupo de desarrollo, los que finalmente tendrán la voz dentro del ámbito de seguridad del producto que se está desarrollando. Un Security Champion tiene como deber asegurarse de que la seguridad no es un bloqueo en el desarrollo activo del software, además de ayudar en los procesos de QA & Testing, definición de pruebas y concientizar sobre la importancia de la seguridad de la información, con fuentes de otras organizaciones como OWASP. Es importante considerar que se debe invertir en una buena capacitación en los colaboradores, con el fin de desarrollar un buen personal de seguridad, por tanto, las organizaciones deben proporcionar nuevas contrataciones con las capacitaciones y herramientas adecuadas para contribuir al desarrollo de un software seguro. Cabe destacar que las capacitaciones siempre deben estar enlazada con los objetivos, políticas y estándares de la compañía para un software seguro.

Procesos

Generalmente, los procesos en una empresa se dividen en distintos grupos, los cuales suelen no estar interconectados con otros, lo que no es productivo para la organización. Por tanto, esta metodología busca alinear e implementar procesos comunes en la empresa para facilitar la cooperación entre los distintos grupos, como también lograr procesos de desarrollo más seguros. Entre estos procesos se encuentran:

- Integración de Procesos: La integración de la seguridad de la información en los desarrollos agiles debe comenzar desde la etapa de la especificación de requisitos, con la finalidad de reducir el costo de implementar seguridad después de lanzado el producto, por tanto, se recomienda definir requisitos de seguridad y chequear estos en el momento de integración.
- Arquitectura de Seguridad: La arquitectura de seguridad se basa en un conjunto de principios definidos por la organización, estos dependen del tipo de dato que se esté procesando, aunque pueden entregarse principios más generales con tal de guiar el software a un desarrollo seguro. La idea en esta metodología es codificar estos principios, con tal de incluirlos en la arquitectura de seguridad de la empresa.
- Gestión de incidentes: Es importante que se tengan definidos previamente planes de acción frente a incidentes de seguridad, con tal de asegurar que la respuesta frente a un incidente sea consistente, repetible y medible, para así finalmente automatizar estos planes de acción.
- Equipos Rojos y recompensa de bugs: Las organizaciones deben tener un equipo rojo, los encargados de cazar amenazas, demostrando las amenazas que puedan existir y planteando una solución, para así entregarle una retroalimentación de seguridad a los desarrolladores. Además, las empresas deberían de vez en cuando poner en práctica programas de recompensa de vulnerabilidades para encontrar e informar fallos en el software.
- Inteligencia de amenaza: Similar a los equipos rojos, Inteligencia de amenaza debe comparar los datos de inteligencia de amenaza obtenidos de proveedores externos y actualizar los planes de acción automatizados ya existentes.

Tecnologías

Las tecnologías son las que permiten a los colaboradores ejecutar correctamente los procesos de DevSecOps. Entre estas tecnologías necesarias se encuentran:

- Automatización y Gestión de la Configuración: La automatización y la orquestación hacen más fácil el proceso de auditoría, como el uso de plantillas de configuraciones, el que ayuda a implementar la trazabilidad entre cada cambio en un código con su configuración, por lo que así es más fácil identificar la causa raíz de un problema.
- Seguridad como código: Se debe estar constantemente actualizando los estándares de codificación según las recomendaciones de seguridad actuales como las que ofrece “OWASP Top 10”. Además, se debe verificar y probar el código, independiente de que exista un cambio muy pequeño.
- Auditorías y exploración de nivel de aplicación: Se debe utilizar diversas soluciones que ayude a detectar fallas o potenciales problemas en el código, para así darle una mayor garantía de seguridad al software. Entre estas tenemos la utilización de IDE junto a un plugin de análisis de código, auditorías previas y posteriores a la implementación, entre otros.

La utilización de esta metodología será para extraer algunas ideas de buenas prácticas que recomienda DevSecOps para incluir la seguridad de la información en una metodología ágil.

2.1.3. ISO 27001-2

Según el informe “ISO 27001 – Aspectos claves de su diseño e implementación” de la consultora ISOTools, define la norma ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) que describe cómo gestionar correctamente la seguridad de la información en una organización (ISOTools, 2017). Para esto, esta norma establece los requisitos necesarios para definir, implementar, mantener y mejorar de manera continua un Sistema de Gestión de la Seguridad de la Información (SGSI). Además, en conjunto con la ISO 27002, incluye los controles para la evaluación y tratamiento de los riesgos asociados a la seguridad de la información, divididos en 2 grandes objetivos: políticas de seguridad de la información y controles operacionales. Cabe destacar que en la ISO 27001:2005 se presentaban 133 controles para los riesgos, mientras que en la versión 2013 se redujo a 113.

Las fases para el desarrollo de un SGSI según la norma ISO 27001 son:

1. Definición de un plan de control o mejora frente a los riesgos: Realizar un plan de control para cada riesgo, incluyendo su criticidad y método para afrontar este, ya sea, eliminarlo o mitigarlo.
2. Alcance de la gestión: Definir el alcance de un SGSI en una organización, por ejemplo, definir en qué áreas de la empresa se desea implementar primeramente priorizando las más críticas.
3. Contexto de la organización: Determinar los problemas internos y externos de la organización, así como sus debilidades, posibles amenazas, fortalezas y oportunidades que pueden afectar a la compañía.
4. Partes Interesadas: Comprender y analizar las necesidades y expectativas de todas las partes interesadas de la organización.
5. Fijación y medición de Objetivos: Definir objetivos medibles para la gestión de riesgos, además de incluir indicadores que permitan realizar seguimientos de estos.

6. Análisis y evaluación de riesgos: Identificar las amenazas internas y externas que puedan afectar a la información, además, analizar el impacto y las consecuencias para la organización.
7. Implementación de Controles: Seleccionar los controles que permitan cubrir y auditar a futuro cada riesgo identificado previamente.
8. Proceso de documentación: Gestionar eficazmente los documentos internos (políticas internas, documentación de proyectos, etc.) y externos (correspondencias, etc.), mediante la aplicación de un método sistemático para su manejo, así como también la redacción de un procedimiento para su gestión.
9. Auditorías: Realización periódicamente de auditorías internas para comprobar la gestión del SGSI, como sus controles. Además, debe resolver las no conformidades detectadas por el grupo de auditoría, con tal de tener una mejora continua en su sistema SGSI.

La utilización de esta norma en el trabajo actual se enfocará en la extracción de las políticas y controles más relevantes a contemplar en el resguardo de la seguridad de la información. Además, para este proyecto, se utilizará la versión del año 2013 de esta norma. En el anexo A3 se especificarán las políticas y controles de seguridad entregados por esta norma.

2.1.4. PCI-DSS

El estándar de seguridad de datos para la industria de tarjetas de pago (PCI-DSS) se define como un conjunto de controles de seguridad que las empresas que trabajen con datos de tarjetas de pago deben implementar y cumplir (Rouse, 2012). Los 12 requisitos que deben cumplir las organizaciones son:

1. Instalar y mantener una configuración de firewall para proteger los datos de los titulares de estas tarjetas de pago.
2. No utilizar los valores predeterminados tales como contraseñas y otros parámetros de seguridad suministrados por el proveedor.
3. Proteger los datos almacenados de los titulares de tarjetas.
4. Cifrar los datos de los titulares de tarjetas transmitidos a través de redes públicas.
5. Usar y actualizar regularmente el software de antivirus utilizado.
6. Desarrollar y mantener sistemas y aplicaciones seguras.
7. Limitar el acceso a los datos de los titulares, únicamente a los datos que los negocios necesitan saber de estos.
8. Asignar una identificación única a cada persona con acceso a un computador.
9. Restringir el acceso físico a los datos de los propietarios de tarjetas.
10. Rastrear y monitorear todo el acceso a los recursos de la red y a los datos de los propietarios de tarjetas.
11. Probar con regularidad los sistemas y procesos de seguridad.
12. Mantener una política que aborde la seguridad de la información.

En el anexo A4 se encuentran los distintos controles que ofrece el estándar PCI-DSS v3.2. La utilización de este estándar en el proyecto se enfoca a extraer los controles de seguridad más relevantes que permitan el desarrollo de software capaz de resguardar la seguridad de la información. Cabe destacar que para este proyecto se utilizará la versión PCI-DSS v3.2.

2.1.5 OWASP Top 10

Es un documento de los 10 riesgos de seguridad más importantes en las aplicaciones web según OWASP, con el objetivo de educar a los desarrolladores, diseñadores, arquitectos, gerentes y organizaciones en sí sobre las consecuencias de las distintas vulnerabilidades de seguridad (OWASP, 2017). Para esto, se recopilan las vulnerabilidades de diversas empresas para sacar las 10 más importantes priorizadas por explotabilidad, detectabilidad e impacto, y así ofrecer técnicas básicas de cómo protegerse de estas, así como los pasos a seguir para realizarlo.

En este trabajo, este documento se utilizará para extraer información sobre las distintas vulnerabilidades, las que pueden ser abordadas en el plan de sensibilización.

2.1.6 Plan de Sensibilización

Según la ISO 27001, un plan de sensibilización o concientización consiste en la planificación mediante un calendario de una serie de actividades con el fin de educar sobre la seguridad de la información e ISO27001 mediante el uso de videos, debates, charlas, etc. (ISOTools, 2014). Para esto, primero es necesario estudiar las necesidades de la organización. Luego, para concientizar a los colaboradores, se debe conocer que necesitan, para esto se puede utilizar actividades como encuestas para analizar problemas, reuniones, la política de seguridad e información sobre otros incidentes. Para la definición del plan, este debe incluir diversos elementos como:

- A quien va dirigido el plan.
- Ley o norma que obligue a la concientización de los colaboradores en materia de seguridad de la información (en caso de que exista).

- Objetivos medibles para cada apartado del plan, con la finalidad de medir si las tareas que son ejecutadas han sido efectivas o no.
- Instrucciones y medios del cómo se va a concientizar.
- Definición de la frecuencia con que se realizarán estas actividades, ya que, la sensibilización no es algo que pueda enseñarse con una sola actividad de concientización.

Finalmente se planifica las actividades en un calendario y se prepara el material a utilizar. Entre los aspectos que se pueden abordar en estas actividades se tienen temas como el uso de contraseñas, protección contra virus, respetar políticas de seguridad y software permitidos y no permitidos, entre otros.

En el proyecto, se utilizará un plan de concientización para proveer conocimientos sobre la importancia de la seguridad de la información en una organización y principalmente en el software/aplicación que se esté desarrollando. En el anexo A2 se presenta un plan de concientización contemplado para un periodo anual, divido por meses, en el cual se entregan posibles temas que pueden ser abarcado en cada mes, junto con una respectiva evaluación para medir la enseñanza entregada a los colaboradores, junto con un incentivo a las mejores calificaciones en estas, la que debe ser definida por la organización que esté aplicando el plan.

2.1.7 Ethical Hacking

Se conoce como Hacking a una técnica de modificación de las características de un sistema. Mientras que la persona que está involucrada en estas actividades se denomina Hacker. A partir de esto, según el artículo “Study of Ethical Hacking” de la editorial International Journal of Computer Science Trends and Technology (IJCST), el Ethical Hacking, también conocido como “Penetration Hacking”, “Intrusion Testing” o “Red Teaming”, es definido como la práctica de hackear el sistema sin malas intenciones,

realizado por un experto en seguridad con conocimientos de hacking, con el fin de evaluar la seguridad del sistema, reportar las vulnerabilidades y dar instrucciones de como remediar con estas (Sahare, Naik, & Khandey, 2014). En un Ethical hacking, existen 3 test de seguridad, estos son:

- Black-box: No se posee conocimiento de la infraestructura que se está evaluando.
- White-box: Se posee un conocimiento completo de la infraestructura que se está evaluando.
- Gray-box: Se evalúa el sistema desde el interior.

Esta técnica tiene como beneficio proporcionar una evidencia de las amenazas del sistema, lo cual, a pesar de ser negativo el encontrar una vulnerabilidad, proporciona la posibilidad de mejorar continuamente en la seguridad del sistema para evitar ataques por estas brechas. Sin embargo, no es la mejor técnica, debido a que solo se enfoca en encontrar formas de penetración en el sistema, pero no visualiza distintos problemas o bugs menores que a futuro se puedan convertir en un riesgo de ataque. Además, el tiempo y el costo es un factor crítico para esta técnica, debido a que se requiere encontrar las vulnerabilidades rápidamente para solucionarlas completamente o para mitigarlas.

Existen diversas compañías que realizan este proceso, entre estas se encuentran:

- Dreamlab: Compañía de origen suizo, enfocado en la seguridad de TI, ofreciendo soluciones de ciberseguridad. Entre los servicios que ofrece es auditorías mediante pruebas de penetración, consultorías de seguridad, análisis forense entre otros (Dreamlab Technologies, s.f.).
- ITsec: Empresa dedicada a la consultoría en seguridad de la información y soluciones de seguridad informática, la que ofrece distintos servicios como Ethical hacking. Entre sus principales clientes se encuentra Transbank, Banco Estado, Latam Airlines, AFC Chile, entre otros (ITSec, s.f.).

El uso de esta técnica en el presente proyecto es con la finalidad de que las organizaciones o el grupo de trabajo haga uso de un Ethical hacking, con tal de hallar las vulnerabilidades más críticas en el sistema desarrollado, y solucionarlas previo a la puesta en marcha del software final.

2.1.8 Escáner de Vulnerabilidades

Según el artículo “Vulnerability Scanners: A proactive approach to assess Web Application Security” de la editorial International Journal on Computational Sciences & Applications (IJCSA), un escáner de vulnerabilidades es un software capaz de detectar las vulnerabilidades en un sistema y clasificarlas según el impacto que puede generar en: criticas, alta, media, bajo e información (Bairwa, Mewara, & Gajrani, 2014). Estos generalmente se utilizan para escanear la red u aplicaciones/software. Existen diversos tipos de escáner para detectar estas brechas de seguridad, entre estos:

- Escáner de aplicación: Es utilizado para evaluar una aplicación específica en la red para encontrar las debilidades de esta, que pueden ser utilizadas a futuro para dañar el sistema.
- Escáner de vulnerabilidades: Es utilizado para descubrir las brechas de seguridad en todo el sistema, las que pueden poner en riesgo a toda la red en caso del acceso de una persona maliciosa.

Algunos softwares que ofrecen servicios de escáner de vulnerabilidades son:

- Nessus: Software de escáner de vulnerabilidades de sistemas, de la empresa Tenable, el que se caracteriza principalmente por escaneo con credenciales, a nivel interno (accediendo con un host al sistema) y externo (se buscan brechas de seguridad a nivel externo como de la vista de un hacker o persona maliciosa (Tenable, 2018). Este software permite el escaneo de vulnerabilidades de

dispositivos de red (firewall, routers, switches, etc.), VMs, bases de datos, sistemas operativos, como también, detecciones de amenazas por malware, procesos maliciosos, Botnet, entre otros.

- APPscan: Software de escaneo de vulnerabilidades de la empresa IBM, (adquirido durante este año 2019 por la empresa HCL Technologies), enfocado a aplicaciones web, el que tiene la capacidad de realizar pruebas de seguridad automatizadas (black-box y White-box) constantemente para detectar diversos problemas de seguridad, además de entregar remediaciones para estas brechas, como parches o listas de tareas y ejemplos de código en caso de ser necesario para su solución (HCL Software, 2019). Así también, entre sus otras versiones ofrece escaneo del código fuente para encontrar vulnerabilidades previo al despliegue de un producto/servicio (HCL Software, 2019), como también generar reportes de estas vulnerabilidades, para ser gestionadas rápidamente.
- ImmuniWeb: Software de escaneo de vulnerabilidades, el cual, junto con integración de Inteligencia Artificial, es capaz de monitorear 24/7 la seguridad del sistema, identificando las brechas de seguridad que existan o puedan generarse, y a la vez, ofrecer parches o guías de remediación para estas brechas (HTBridge, s.f.).

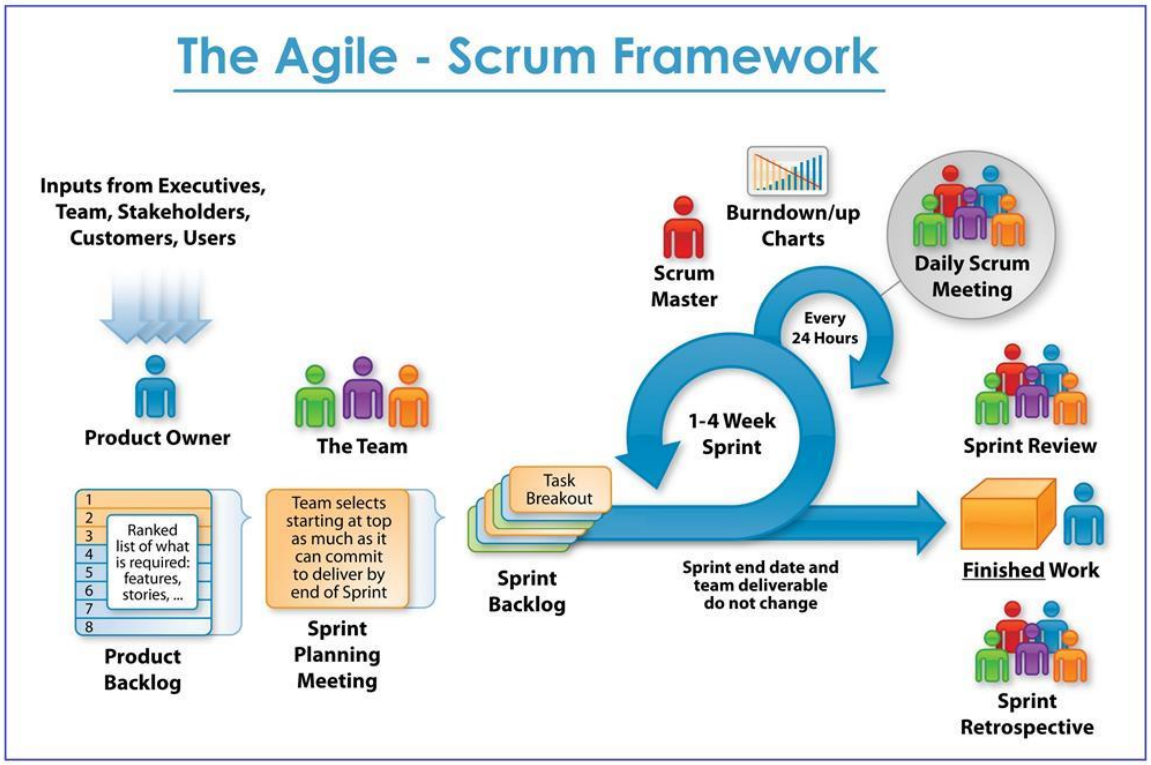
Al igual que la técnica de Ethical hacking, los escáneres de vulnerabilidades en el proyecto actual, será utilizado para encontrar todo tipo de vulnerabilidades que no fueron encontradas con Ethical hacking, como las que no tienen un impacto alto, pero, sin embargo, pueden tener un alto riesgo en un futuro.

2.1.9 Scrum

Según el documento The Scrum Primer", Scrum es una metodología de trabajo iterativo e incremental, la cual estructura el desarrollo del proyecto en ciclos de trabajos llamados Sprint, donde a cada Sprint se asigna un tiempo definido entre 1 a 4 semanas,

con fecha de inicio y término (Deemer, Benefield, Larman, & Vodde, 2010). El Sprint termina en la fecha definida independientemente si se cumplieron o no las Actividades definidas para éste. Al terminar un Sprint comienza inmediatamente El siguiente. Al inicio de cada Sprint, el equipo selecciona los requisitos desde una lista priorizada definida al inicio del proyecto (Pila del Producto o Product Backlog), para así crear la lista de objetivos y requisitos del Sprint (Pila del Sprint o Sprint Backlog). Todo lo que incluye la Pila Del Sprint son los requisitos y/o objetivos que el equipo se compromete a realizar Durante el Sprint, donde dicha lista no podrá cambiar durante el Sprint. Todos los días se realizan breves reuniones de pie con todos los integrantes del equipo para Informar sobre los progresos y problemas que se encuentran del día anterior de trabajo. Al terminar cada Sprint, se debe entregar una parte funcional del producto, la cual es revisada con los interesados del proyecto, para mostrar lo que se ha hecho. En la figura 5 se muestra un pequeño diagrama donde se muestran los roles, Artefactos y eventos principales de Scrum.

Figura 5 – Diagrama de etapas de metodología Scrum



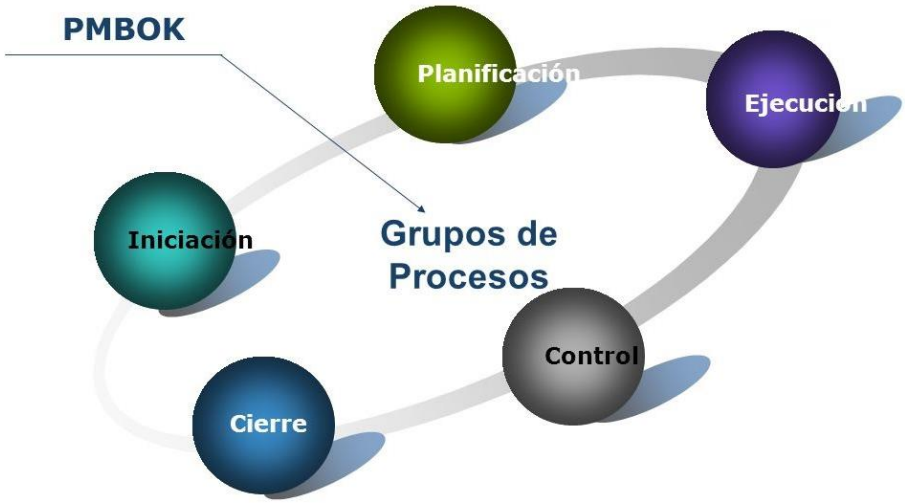
Fuente: (Deemer, Benefield, Larman, & Vodde, 2010)

En relación con la figura 5, se puede visualizar el framework de la metodología Scrum, en la que se encuentra el Dueño del Producto, quien es el encargado de gestionar la Pila Priorizada del Producto, para que el equipo implemente primero las funcionalidades que tienen mayor prioridad. Esto lo hace con el objetivo de maximizar las ganancias, ya que es el responsable de las pérdidas y ganancias del proyecto en el caso de ser un producto comercial. En caso de que no sea un producto comercial, es el encargado de gestionar la Pila del Producto de manera que se realicen en primer lugar los requisitos que le generen mayor valor de negocio al producto. Luego se encuentra el Scrum Master que, en resumen, es la persona encargada de guiar al Equipo y al Dueño del producto para aplicar de manera correcta la metodología y conseguir el éxito en el proyecto. El Scrum Master sirve al equipo, no debe ser visto como un jefe del equipo o del proyecto. Deemer, Benefield, Larmann y Vodde señalan que “El Scrum Master se asegura de que todo el mundo en el equipo (incluyendo al DP y la gerencia) entienda y siga las prácticas de Scrum, y ayuda a llevar a la organización, a través de los cambios necesarios y frecuentemente difíciles, a conseguir el éxito con el desarrollo ágil” (Deemer, Benefield, Larman, & Vodde, 2010).

2.1.10 PMBOK

La metodología o guía del Pmbok, es una herramienta desarrollada por el Project Management Institute (PMI), la que entrega un criterio de buenas prácticas relacionadas con administración, dirección y gestión de todo proyecto (Retos en Supply Chain, 2017), implementando diversas técnicas y herramientas divididos en 49 procesos, los que a su vez se agrupa en 5 macroprocesos, como se verá en la figura 6 a continuación.

Figura 6 – Procesos de metodología Pmbok



Fuente: (Ruiz, Zulueta, & Gainza, 2007)

Como se puede visualizar en la figura anterior, según la guía Pmbok, identifica 5 procesos principales en los que se agrupan todos los procesos definidos como estándares en todo proyecto:

1. Inicio: Se basa en los procesos cuyo fin es definir un nuevo proyecto o una nueva fase de ejecución de este, mediante la creación de un acta de iniciación de un proyecto, así como también obtener la autorización para ser llevado a cabo.
2. Planificación: Este macroproceso se basa al establecimiento de objetivos y alcances del proyecto, y al diseñar las estrategias adecuadas para lograr su desarrollo.
3. Ejecución: Este macroproceso incluye diversos procesos enfocados al correcto desempeño, de acuerdo con la estrategia adoptada de las actividades definidas para el desarrollo del proyecto.
4. Control y monitorización: En este macroproceso se incluye todo proceso relacionado con la supervisión y evaluación del desempeño del proyecto.
5. Cierre: En este último macroproceso, se incluyen aquellos procesos que cierran en su totalidad el proyecto, o alguna fase de este, el cual hace referencia al grado de aceptación con el resultado obtenido del proyecto.

Asimismo, en cada macroproceso intervienen 10 áreas del conocimiento en los que se basa principalmente esta metodología:

1. Integración: Área relacionada con la dirección de proyectos, definiendo criterios para una correcta gestión, administración y coordinación de los distintos procesos y actividades implicadas en los proyectos.
2. Alcance: Relacionado con la definición del alcance del proyecto, junto con todas las actividades implicadas en estos.
3. Tiempo: Gestión del tiempo de ejecución de las actividades y procesos y monitorización para cumplir con los tiempos establecidos.
4. Costos: Gestión de los costos del proyecto y control de estos para velar que no supere la presupuestación inicial.
5. Calidad: Se basa en la determinación de responsabilidades en la obtención de resultados de las actividades y procesos implicados en el proyecto. Además, establece las políticas de calidad a las que debe someterse estos resultados.
6. Recursos Humanos: Gestión del grupo humano implicado en el proyecto y/o en cada fase de este.
7. Comunicaciones: Área responsable de la gestión y administración de los mecanismos, vías y estrategias de comunicación entre las distintas áreas internas del proyecto.
8. Riesgos: Área relacionada a la detección, gestión y solución de los riesgos en cada una de las etapas del proyecto.
9. Adquisiciones: Área de gestión de los procesos de compra de bienes, estructuras, herramientas, servicios externos u otros activos relacionados al desarrollo del proyecto.
10. Stakeholders: Se refiere a la gestión de los interesados o posibles inversores, así como la correcta administración de las expectativas generadas con el proyecto.

2.2 Discusión

Los ciberataques son cada vez más comunes en las organizaciones, existen casos emblemáticos en que se han visto vulnerados los sistemas de estas empresas, accediendo así a datos confidenciales de esta. A continuación, se describirán diversos casos de ciberataques más populares a lo largo de estos últimos años debido a la gran magnitud de afectados.

Saudi Aramco

En el año 2012, la empresa más grande de gas y petróleo del mundo sufrió un ciberataque debido a que un trabajador de esta compañía cometió un error, presionando un enlace corrupto, dando así acceso a la computadora del trabajador, por lo que una vez dentro de la red comenzaron a infectar a todos sus equipos. Se estima que en cuestión de horas dañaron más de 30.000 discos duros correspondiente a los equipos y servidores de la empresa. Para contener el ataque la empresa cortó toda conexión a la red, prescindiendo del uso de la tecnología por un tiempo. Luego frente a esto, la organización optó por botar todos los equipos afectados y reemplazarlos, por lo que decidieron comprar más de 55.000 discos duros, incluso por encima de su precio a cambio por una entrega inmediata, afectando así al mercado mundial, ya que desabasteció los mercados, por lo que incrementaron los precios a nivel mundial (Rios, 2016).

eBay

En el año 2014 eBay admitió haber sufrido un ataque por parte de un grupo de hackers del cual se extrajo una base de datos cifrada, en la que se almacenaba las contraseñas de todos sus usuarios, afectando así a 145 millones de usuario. Sin

embargo, esta base de datos no poseía los datos asociados a cuentas bancarias y cuentas de PayPal, pero igualmente fue duramente criticada por los usuarios, debido a que solo colocaron un pequeño mensaje en el sitio web, recomendando a los usuarios cambiar su contraseña debido al ciberataque, y no enviar un correo electrónico que advierta de lo sucedido (Peña, 2017). Por esta razón y por la cantidad de usuarios a los que comprometió se considera uno de los ataques más grandes de la historia.

Sony Pictures

En el año 2014 la firma Sony Pictures sufrió un ataque que comprometió más de 100Tb de datos, entre las que se robó películas no estrenadas, además de información sobre guiones e información sobre proyectos futuros. Los daños afectados para la compañía se estimaron en un alrededor de 100 millones de dólares (Peña, 2017).

Ashley Madison

En el año 2015, el sitio de citas sufrió un ciberataque por un grupo de hackers, la que ha dejado expuestos a información confidencial de más de 37 millones de usuarios, exponiendo así datos como los nombres de los usuarios, datos de tarjetas de créditos, correos electrónicos relevantes, características físicas, fotografías y hasta conversaciones de estos usuarios (HuffPost, 2015). Cabe destacar que en el año 2012 el mismo fundador de Ashley Madison advirtió a sus colegas el riesgo de un posible ciberataque por no contar con un SGS, y a pesar de esto, la empresa comenzó a trabajar entre el año 2014 y 2015 en la seguridad de su sistema, cuando estos recibieron la amenaza del grupo de hackers.

Vulnerabilidad del Banco de Chile

Durante una charla de seguridad realizada en el OWASP LATAM TOUR 2018, realizada por el estudiante de Ingeniería en Informática Eduardo Riveros, reportó una grave vulnerabilidad del Banco de Chile, la cual permitía a los clientes realizar compras en línea por medio de WebPay con una cuenta de otro cliente con solo conocer su Rut (Hevia & Riveros, 2018). Esto se debía principalmente al mecanismo de autorizaciones digital de transacciones "Mi Pass", el que según el estudiante explica, al realizar la solicitud de operación desde el portal del banco, este envía un archivo en formato JSON a el banco, el que luego le enviaba un mensaje al dispositivo móvil para autorizar esa operación, para luego asignarle una id de autorización. Luego al realizar cualquier otra operación con esta id entregada anteriormente, se autorizaba cualquier otra operación, incluso sin la vinculación de un dispositivo móvil para estas autorizaciones. Finalmente, se realizó la prueba de cargar una compra a otro cliente, en la que se realizaba una compra mediante WebPay, ingresando un Rut de otro cliente, para luego en el portal del banco cambiar el Rut ingresado en WebPay por las credenciales de otro cliente conocido, para luego realizar la compra, la que finalmente es cargada en la cuenta asociada al Rut ingresado en WebPay. El último reporte entregado por este grupo de estudiantes al banco fue el 28 de marzo, a la que estos respondieron el 23 de abril asegurando haber resuelto estos problemas.

Como se puede ver en los ejemplos anteriores, los principales grandes ataques y vulnerabilidades pertenecen a compañías Bancarias o proveedoras de algún servicio. Sin embargo, la seguridad de la información no solo se basa en el desarrollo de las aplicaciones bancarias, también puede incluirse en otros ámbitos, como el desarrollo de videojuegos. En el ámbito de videojuegos, un experto dice "la seguridad tiene que considerarse desde el momento en que comienzas a tomar información de tus jugadores, como e-mail, acceso a Facebook, y más aún cuando tu modelo de negocio se asocia a la compra de ítems pagados o monedas virtuales (micro transacciones)". Además, se refiere al desconocimiento de la seguridad en estos sistemas, diciendo "Creo que hay

mucho desconocimiento sobre la seguridad que implementan las compañías de videojuegos. Sin ir más lejos, Sony tuvo comprometida su plataforma online de PlayStation. Hay mucho trabajo que hacer, pero ocurre que al haber tantos juegos es lógico que los desafíos se centren en los juegos más grandes y de compañías famosas" (Sassone, 2016).

Debido a problemas como los expuestos, es en el que se ve la necesidad de proveer una metodología capaz de enmarcar la importancia de la seguridad de la información y el desarrollo seguro de aplicaciones, sobre todo en la actualidad, donde el desarrollo ágil es muy frecuente en sistemas de carácter "no críticos". Sin embargo, a veces, no se visualiza correctamente los riesgos que puede generar el robo de información del negocio, como en el caso de los videojuegos, en el que a veces suelen comprometerse tarjetas bancarias.

En el 2015, un estudiante de la Universidad Politécnica de Cataluña desarrolló una metodología de desarrollo seguro, junto con una aplicación para la facilitar la aplicación de esta metodología llamada S2D2 (Lopez Provencio, 2015). Esta consiste en la correcta gestión en el ciclo de vida del software según CISA, las cuales son: análisis de requisitos y viabilidad, infraestructura y comunicaciones, metodologías de desarrollo, implementación, auditoría, despliegue, monitorización y mantenimiento. En cada etapa del desarrollo, se dan a conocer todos los controles que se deben considerar, según los aportados por CISA, OSSTMM e ISO27001:2005. Su aplicación en tanto permite comenzar un proyecto y elegir las fases del proyecto que se desea controlar, de las que luego se disponen los controles asociados a estas etapas con la descripción, la importancia de este y el tiempo estimado para llevarlo a cabo. Además, se pueden supervisar estos controles, indicando la fecha de inicio de estos controles, horas dedicadas, fecha de finalización de estos, etc., lo que permite finalmente visualizar la gráfica del progreso de estos controles a lo largo del tiempo. A continuación, se verá una tabla comparativa que resume la diferencia con la metodología mencionada junto con la propuesta actual del presente documento.

Tabla 3 – Comparación de soluciones propuesta

Característica	S2D2	Propuesta Actual
Concientización del personal sobre la importancia de la seguridad de la información	X	✓
Interfaz gráfica para el seguimiento de la metodología	✓	✓
Enfocado a la seguridad de la información en el desarrollo ágil de software	X	✓
Provee checklist con los controles mínimos que debe contemplar un desarrollo seguro de software	✓	✓

Fuente: Elaboración Propia

Como se puede visualizar en la tabla comparativa, uno de las principales diferencias entre la otra metodología propuesta con su aplicación “S2D2”, es que esta no se enfoca en la concientización de los colaboradores sobre la importancia de incluir la seguridad de la información en el desarrollo de un software, sino más bien se basa simplemente en el cumplimiento de los controles en cada etapa del desarrollo de software, cubriendo así solo las brechas o posibles fallos de seguridad que abarcan estos controles entregados. Asimismo, ambas proveen un conjunto de controles a contemplar en el desarrollo de software, sin embargo, S2D2 incluye todos los controles, priorizando como los más importantes a los menos importantes, pero no contempla solo los más relevantes para un desarrollo seguro y ágil. Por otra parte, esta otra metodología no se enfoca en los desarrollos de software ágiles, sino más bien, lo que busca es monitorear la realización de los controles que se entregan para cada etapa del software.

CAPÍTULO III – ENFOQUE METODOLÓGICO

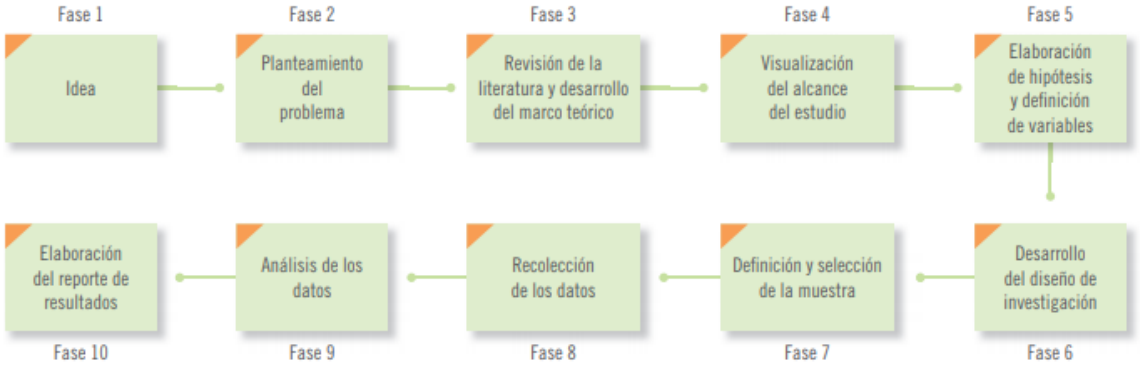
3.1 Enfoque Metodológico

Como metodología de trabajo, se utilizará la Metodología de Investigación Científica Cuantitativa. Se seleccionó esta metodología sobre otras, como por ejemplo PMBOK, debido a las características del proyecto, debido a que su alcance es de carácter teórico, por lo que no requiere una mayor gestión de otras partes para su desarrollo. A continuación, para entender en que consiste esta metodología, se procederá a explicar cada una de sus fases, basado en el libro “Metodología de la Investigación”, Quinta edición, de Carlos Fernández Collado y Roberto Hernández Sampieri (Hernández Sampieri, Fernández Collado, Baptista Lucio, Méndez Valencia, & Mendoza Torres, 2014).

3.2 Metodología de Investigación Cuantitativa

El enfoque científico cuantitativo es una metodología secuencial y probatoria, la cual cada etapa precede a la otra, por tanto, no es posible eludir alguna de estas fases. Este enfoque, se basa en un conjunto de fases, el que comienza desde una idea general, la cual se va acotándose hasta encontrarse lo suficientemente delimitada, para así generar preguntas de investigación y objetivos de acuerdo con la revisión de la literatura. Así finalmente, se establece la hipótesis a verificar junto con las variables intervenidas las cuales se miden en un contexto determinado, mediante el plan de diseño de investigación, para así establecer las conclusiones respecto a la hipótesis verificar. En la siguiente figura, se visualizará en mayor detalle cada fase, junto con una explicación en mayor profundidad.

Figura 7 – Fases Metodología de Investigación Científica Cuantitativa



Fuente: (InfoeducativaDigital, 2017)

Como se puede visualizar en la figura anterior, se comienza con la fase de inicio de la investigación o proyecto, en la cual se presenta la realidad de la cual se desea estudiar. En la fase dos, luego de la investigación en la literatura sobre el tema a desarrollar, se plantean el problema de investigación, se establecen sus objetivos y las preguntas que se buscan responder. En la fase tres, se revisa la literatura relacionado al problema planteado, y se construye el marco teórico, con tal de generar una inmersión en el conocimiento actual sobre el problema planteado. Además, se revisa si existen otros intentos de abordar la problemática y el estado actual en caso de existirlo. En la fase cuatro, se debe elegir el alcance de la problemática a investigar, este alcance puede ser de 4 tipos:

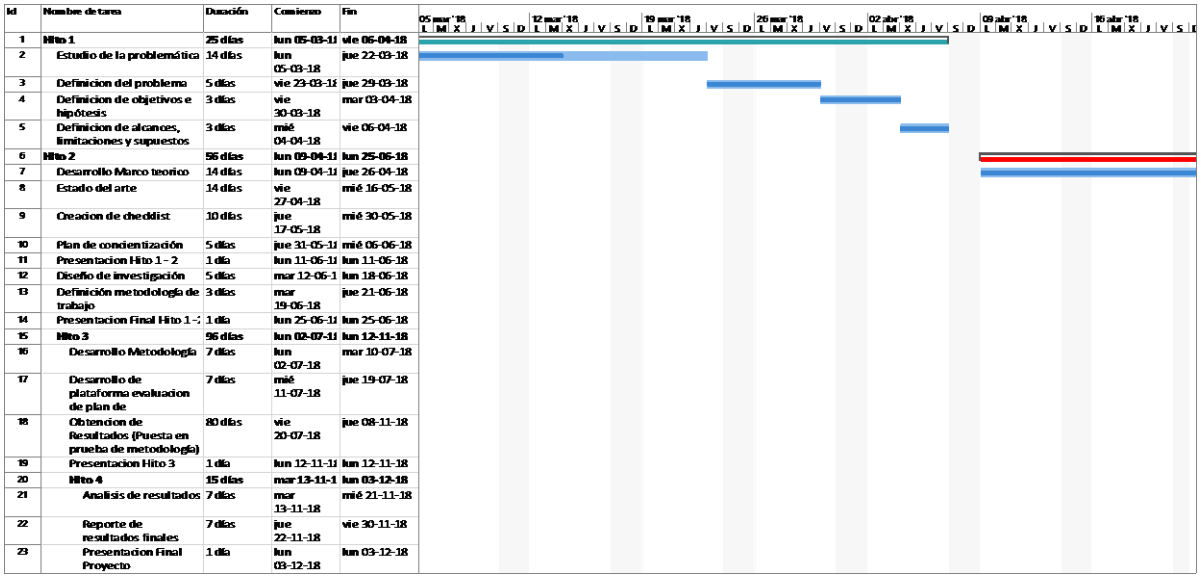
- Exploratorio: Se utiliza cuando el objetivo es examinar un tema o problema de investigación poco estudiado o no abordado nunca.
- Correlacional: Buscan responder preguntas de investigación asociadas a un comportamiento u patrón en un grupo o población.
- Descriptivo: Buscan especificar características, propiedades o perfiles de personas, grupos, comunidades, procesos, o cualquier otro proceso que se someta a un análisis.
- Explicativo: Están dirigidos a responder preguntas sobre causas asociadas a eventos y fenómenos físicos o sociales.

En la fase cinco, se define la finalidad del estudio, así como las variables que permitirán medir y asimismo validar el estudio. En la fase seis, se debe diseñar el experimento a realizar, junto con el contexto en el cual será aplicado, con el fin de medir las variables previamente definidas. En la fase siete, se deben definir las entidades que intervienen y depende el estudio que se evaluará, tal como la definición de la población en la cual se llevará a cabo, se elige el método de selección de la muestra (ya sea probabilístico o no probabilístico), el tamaño de la muestra, proceso de selección y obtención de esta muestra. En la fase ocho, se recolectan los datos pertinentes sobre las variables de análisis, basado en el desarrollo de un plan para obtener estos datos. En la fase nueve, se realiza el análisis e interpretación de los datos obtenidos en la fase anterior. Finalmente, la última fase se encarga en la realización de un reporte para presentar el análisis de los datos obtenidos en la fase anterior para ser presentados. Este reporte puede llevarse a cabo mediante una presentación, un artículo para una revista, un documento técnico, entre otros.

3.3 Gestión del Tiempo del Proyecto

Para la gestión del tiempo del proyecto actual, se utilizará una Carta Gantt para definir las distintas tareas a realizar junto con su estimación en días, la que se podrá visualizar en la figura a continuación.

Figura 8 – Carta Gantt



Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Hito 1**	25 días	lun 05-03-18	vie 06-04-18
2	Estudio de la problemática	14 días	lun 05-03-18	jue 22-03-18
3	Definicion del problema	5 días	vie 23-03-18	jue 29-03-18
4	Definicion de objetivos e hipótesis	3 días	vie 30-03-18	mar 03-04-18
5	Definicion de alcances, limitaciones y supuestos	3 días	mié 04-04-18	vie 06-04-18
6	**Hito 2**	56 días	lun 09-04-18	lun 25-06-18
7	Desarrollo Marco teorico	14 días	lun 09-04-18	jue 26-04-18
8	Estado del arte	14 días	vie 27-04-18	mié 16-05-18
9	Creacion de checklist	10 días	jue 17-05-18	mié 30-05-18
10	Plan de concientización	5 días	jue 31-05-18	mié 06-06-18
11	Presentacion Hito 1 - 2	1 día	lun 11-06-18	lun 11-06-18
12	Diseño de investigación	5 días	mar 12-06-18	lun 18-06-18
13	Definición metodología de trabajo	3 días	mar 19-06-18	jue 21-06-18
14	Presentacion Final Hito 1 - 2	1 día	lun 25-06-18	lun 25-06-18
15	**Hito 3**	96 días	lun 02-07-18	lun 12-11-18
16	Desarrollo Metodología	7 días	lun 02-07-18	mar 10-07-18
17	Desarrollo de plataforma evaluacion de plan de	7 días	mié 11-07-18	jue 19-07-18
18	Obtencion de Resultados (Puesta en prueba de metodología)	80 días	vie 20-07-18	jue 08-11-18
19	Presentacion Hito 3	1 día	lun 12-11-18	lun 12-11-18
20	**Hito 4**	15 días	mar 13-11-18	lun 03-12-18
21	Analisis de resultados	7 días	mar 13-11-18	mié 21-11-18
22	Reporte de resultados finales	7 días	jue 22-11-18	vie 30-11-18
23	Presentacion Final Proyecto	1 día	lun 03-12-18	lun 03-12-18

Fuente: Elaboración Propia

Como se puede ver en la Carta Gantt, se tienen las distintas tareas a realizar durante el proyecto, dividido por 4 hitos. El primer hito, se basa en el estudio de la problemática, como también la definición del problema, objetivos y alcances. Para el hito 2, se realiza estudian los conceptos más relevantes para el proyecto, como también buscar el estado actual de la problemática, para ver si existen otros intentos de solucionar el problema planteado, luego se diseña el plan de investigación (como se obtendrán los datos y que datos se esperan obtener), para finalmente definir la metodología de trabajo del proyecto. En el caso del hito 3, se comienza el desarrollo de la metodología, junto con el desarrollo de una plataforma para la evaluación de la concientización hacia los trabajadores, para finalmente poner a prueba a la metodología y así obtener los resultados. Finalmente, para el hito 4, se termina con el análisis de resultados, el reporte final de los resultados con su respectiva documentación, y finalmente la presentación final del proyecto.

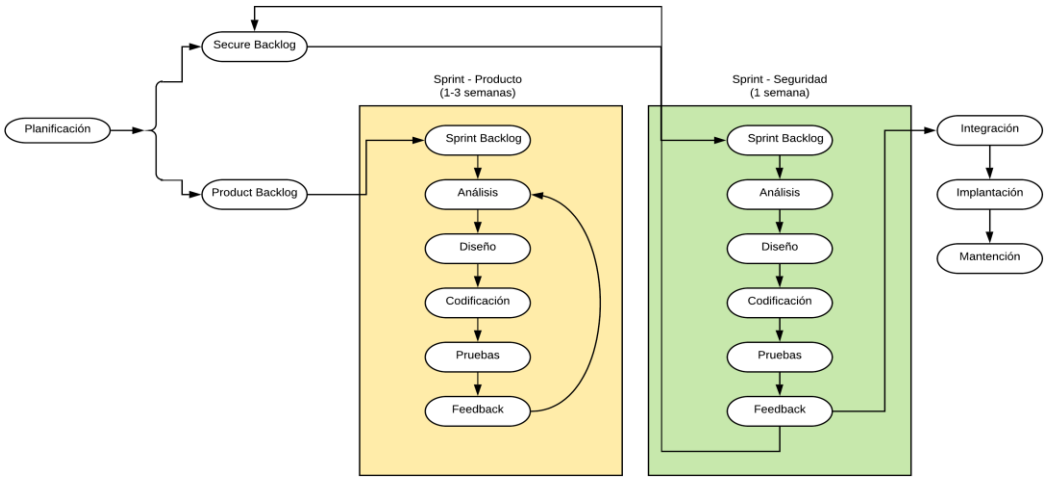
CAPÍTULO IV – DESARROLLO DEL PROYECTO

En el presente capítulo se dará a conocer la metodología de desarrollo seguro de software propuesta, junto con una descripción de cada una de sus etapas.

4.1 Metodología Propuesta

La metodología de desarrollo seguro de software a entregar se basará en 2 metodologías ya conocidas: Scrum y PMBOK. Asimismo, se hará uso de algunas características de las metodologías entregadas en los capítulos anteriores como DevSecOps y Secure Scrum. Las etapas que se considerarán para el desarrollo de todo proyecto con esta metodología se basarán en las mismas que Scrum, esto quiere decir que se comenzará con una etapa de planificación, terminando esta con un product backlog, pero adicionalmente, se añadirá un secure backlog para comenzar la planificación del sprint y comenzar su realización. A continuación, se mostrará el esquema de la metodología propuesta.

Figura 9 – Esquema metodología propuesta



Fuente: Elaboración propia

En la figura 9 se puede visualizar el esquema de la metodología propuesta, que tal como ya se explicó comienza con una etapa de planificación, ya sea toma de requerimientos, gestión de recursos, tiempo, etc., y acta de iniciación de proyecto. Finalizado esta etapa se obtiene un Product Backlog, y adicionalmente un Secure Backlog, el que al igual que en la metodología de Secure Scrum, incluirá todos los requisitos asociados a la seguridad del sistema. Posteriormente comienzan los desarrollos de los sprints, en el cual, por cada sprint considerado para un proyecto, se considerará un segundo asociado al Secure Backlog, del cual el primer sprint asociado al Product Backlog tendrá una duración estimada de 1 a 3 semanas, mientras tanto el segundo se dará solo una semana. Cada sprint contendrá las etapas de análisis, diseño, codificación, pruebas y feedback. Teniendo en el sprint del producto la posibilidad de volver al análisis para mejorar el desarrollo del módulo actual, mientras que en el de seguridad, lo que resulte del feedback será agregado al Secure Backlog para ser resueltos en una próxima iteración.

4.1.1 Etapa de Planificación

Esta etapa consiste en toda tarea a realizar previo al diseño y desarrollo de las diversas funcionalidades y partes del sistema y/o software a desarrollar. Entre estas tareas se encuentran:

- Estudios previos del caso: Es importante realizar un estudio previo de la propuesta, para saber si existen algunas propuestas similares, sus últimos avances, entre otros, con tal de no reinventar la rueda, cometer errores similares o tener una idea para innovar sobre lo ya existente.
- Toma de requerimientos: Funcionales y relacionados con seguridad del sistema.
- Acta de inicialización del proyecto: Incluye descripción del proyecto, objetivos, alcances, riesgos, historias de usuario, etc.

- Gestión de personal: Se basa en la búsqueda de personal adecuado para el tipo de proyecto se está realizando. En caso de no tener las habilidades y/o conocimientos necesarios, es deseable que se capacite al personal previamente.
- Gestión de recursos: Se basa en la gestión de los recursos (ya sea monetarios, de personal, de hardware y software, entre otros), para tener los implementos necesarios y/o personal adecuado para el desarrollo del proyecto.
- Gestión de tiempo: Es importante gestionar el tiempo estimado para la realización del proyecto, generalmente mediante el uso de una Carta Gantt con el tiempo estimado de cada etapa del proyecto, para al final de este determinar el desempeño que se tuvo durante su desarrollo.

La etapa de planificación termina con la generación del Product Backlog (o Pila del producto) con las tareas que se deberán realizar durante el proyecto priorizadas de las más a menos relevantes. Esta etapa se considera una de las más importantes, ya que es vital definir claramente lo que debe desarrollarse, con tal de que cumpla con las necesidades del cliente y/o usuario final. Además, hay muchas tareas que influyen claramente la “calidad” del desarrollo, por ejemplo, puede verse el caso que debido a una mala aplicación de las tareas en esta etapa se deban redefinir objetivos, alcances, requisitos, etc. lo que influye en un retraso del proyecto, lo que a su vez puede conllevar a un mal desarrollo, inclusive dejando “de lado” algunos de los requisitos de seguridad mínimos del sistema. Durante esta etapa, los diversos actores en un proyecto cumplen distintos roles. En este caso, el jefe de proyecto será el encargado de realizar la toma de requerimientos, así como realizar gran parte del análisis previo junto a diversos analistas, como la definición de objetivos del proyecto, alcances, entre otros. Además, es el encargado de gestionar la contratación de personal, los costos asociados a estos, el tiempo de duración del proyecto, etc. Así también, durante esta etapa, como también en el desarrollo del proyecto, el jefe de seguridad toma un rol muy importante, ya que será el encargado de gestionar el plan de sensibilización a los integrantes del grupo de trabajo, con tal de destacar la importancia de la seguridad de la información y reducir posibles riesgos al momento de comenzar el desarrollo del proyecto. Mientras tanto, el resto de

personal deberá asistir a estas “clases de concientización” para finalmente ser evaluados con preguntas asociadas a diversas situaciones, con tal de dejar clarificado los puntos que se quieren abordar de esta sensibilización. Además, estos tendrán acceso a la plataforma en que podrán visualizar y estudiar los controles relacionados a una buena gestión de la seguridad de la información durante el desarrollo de un proyecto, con tal de ambientarse en lo que deberían o no considerar al momento de comenzar el desarrollo de este.

4.1.2 Sprint Planning

Durante esta etapa el equipo de trabajo debe priorizar las tareas previamente definidas en el product backlog, con tal de realizar las funcionalidades y características de seguridad más importantes y vital para el sistema y/o software que se está desarrollando. Además de gestionar los recursos y tiempos para llevar a cabo estos.

4.1.3 Análisis y diseños(prototipado)

Durante esta etapa, en los sprints, se debe realizar un análisis de las diversas tareas a implementar en determinado sprint, con tal que cumpla con las expectativas del cliente. Además, se realiza un prototipado de estas funciones con tal de ser presentado al cliente para corregirlo a partir del feedback del cliente para finalmente comenzar con su desarrollo. Entre algunas actividades que deben realizarse se encuentran:

- Prototipado
- Casos de uso
- Definición casos de prueba

4.1.4 Desarrollo de Sprint

A partir de lo corregido con la reunión con el cliente sobre el prototipo presentado, comienza el desarrollo del Sprint, tanto de las funcionalidades como requisitos de seguridad, para así realizar las pruebas de funcionalidad y seguridad, para finalmente realizar las pruebas de aceptación con el cliente, y ser integrado en el sistema final.

4.1.5 Integración

Durante esta etapa se realiza la integración de todas las partes realizadas en los diversos sprints, para finalmente realizar pruebas sobre el sistema final con todas sus piezas integradas. Asimismo, se realiza pruebas y presentación final junto con el cliente para así comenzar la implementación del sistema en caso de que lo requiera y así dar cierre al proyecto, dando comienzo a una larga etapa de mantenimiento.

CAPÍTULO V – DESARROLLO PLATAFORMA WEB

A lo largo del presente informe, se presentó una propuesta de metodología de desarrollo seguro de software. Sin embargo, como valor agregado, se desarrolló una plataforma web, la cual se dividió en 2 plataformas distintas, una especialmente para gestionar los controles de seguridad de la información en los diversos proyectos, mientras tanto, la segunda solo se enfocó a la gestión y aplicación del plan de sensibilización. Durante el presente capítulo se dará a conocer la etapa de análisis y desarrollo de la plataforma web, en el cual se expondrán los diagramas de casos de uso, diagramas de secuencias y el modelo de vistas y arquitectura 4+1 de Kruchten. Así también, se describirán los roles y perfiles, como también la interfaz gráfica de la plataforma web.

5.1 Roles y Perfiles

Los perfiles asociados a la plataforma web son los siguientes:

- Administrador: Este tiene acceso al total de ambas plataformas. Entre las capacidades que tiene en la plataforma de gestión de proyectos se encuentra:
    - Crear usuarios.
    - Modificar información de usuarios.
    - Eliminar usuarios.
    - Crear proyectos.
    - Eliminar proyectos.
    - Modificar información de proyectos.
    - Visualizar proyectos.
    - Visualizar y modificar controles asociados al proyecto.
    - Visualizar métricas asociadas a los diversos controles y a los proyectos en específicos.

- Finalizar proyecto.

Para la plataforma de plan de concientización, este tiene acceso a:

- Crear pruebas.
- Eliminar Pruebas.
- Visualizar métricas a nivel general de los usuarios en desempeño de pruebas de concientización.
- Realizar Pruebas.
- Visualizar su perfil, con su desempeño en las pruebas de concientización.

- Jefe de Proyecto: Como ya fue mencionado, el jefe de proyecto tiene gran responsabilidad durante la gestión del proyecto, por lo que su actividad se basa principalmente en la plataforma de gestión de proyectos. Entre las funciones que puede realizar en este se encuentran:
  - Crear Proyectos.
  - Eliminar Proyectos.
  - Modificar información de Proyectos.
  - Visualizar Proyectos.
  - Visualizar y modificar controles asociados al proyecto.
  - Visualizar métricas asociadas a los diversos controles y a los proyectos en específicos.
  - Finalizar Proyecto.

Para la plataforma de concientización, este tendrá los mismos roles que un usuario común (a menos que este mismo sea administrador de la plataforma), estas son:

- Ver pruebas activas y próximas a la fecha, como también realizar pruebas.
- Visualizar su perfil, con su desempeño en las pruebas de concientización.
- Visualizar métricas a nivel general de los usuarios en desempeño de pruebas de concientización.

- Scrum Master: El Scrum Master, similar al jefe de proyecto, se enfoca principalmente en la primera plataforma, en la que entre sus funciones puede realizar:
    - Modificar información de los proyectos, ya sea su descripción, estado actual del proyecto, fecha de término, entre otros.
    - Visualizar proyectos, sus métricas y controles asociados, como también modificar información respecto a algún control en algún proyecto.

Para la plataforma de concientización puede realizar las mismas funciones que un usuario estándar (como un desarrollador).

- Jefe de Seguridad: El jefe de seguridad en la plataforma de gestión de proyectos, será el encargado de visualizar y verificar la correctitud en la información respecto a la adherencia a diversos controles en un proyecto, validando así o no la información sobre este en un proyecto. Entre las funciones que puede realizar en la plataforma se encuentran:
    - Visualizar los diversos proyectos ya creados junto con sus métricas.
    - Visualizar los diversos controles adheridos y no adheridos de los distintos proyectos.
    - Comentar sobre la decisión tomada del grupo de trabajo de adherirse o no a un control, con tal de informar su conformidad o disconformidad con la decisión tomada, para que así en caso de una disconformidad, el grupo de trabajo pueda verificar y corregir esto o apelar a la disconformidad del jefe de seguridad.
    - Aprobar o Desaprobar un control de un proyecto, con tal de proveer información por parte de un experto en seguridad de la información si está correcto o no la decisión tomada por el grupo de trabajo.

Para la plataforma de concientización, al igual que el administrador, el jefe de seguridad tiene un rol fundamental, ya que este será el encargado de gestionar las pruebas de concientización, seleccionando diversos temas ya predefinido, como también crear sus propias pruebas que sean adecuadas para el grupo de trabajo que se espera sensibilizar sobre la importancia de la seguridad de la información, tanto durante el desarrollo del proyecto y en el área de trabajo en que se está desarrollando. Entre las funciones que este puede realizar se encuentran:

- Crear pruebas, ya sea con las categorías ya definidas en el sistema, como también crear sus propias pruebas, con sus propias preguntas y un video que considere útil para la concientización.
- Eliminar pruebas.
- Visualizar el desempeño a nivel general de las diversas pruebas de concientización. En este se podrá visualizar el puntaje promedio, el máximo, mínimo y los 3 usuarios con mejor desempeño en cada prueba (considerando menor tiempo en resolver la prueba, como también la cantidad de preguntas correctas).
- Auditor: El rol del auditor, tiene como principal rol visualizar las métricas y realizar análisis de estos, para así sacar conclusiones relevantes, tanto en el desarrollo de los proyectos (por ejemplo la baja adherencia de algún control en específico a nivel general en gran parte de los proyectos, lo que puede indicar que el grupo de trabajo no tiene conocimiento sobre lo que se requiere en el control o no saben cómo aplicarlo correctamente al proyecto), como en el plan de concientización (bajo promedio o algunos usuarios con 0 puntajes, lo que puede indicar que el tema que se intentó sensibilizar no se entendió correctamente por el público objetivo).
- Desarrollador: El desarrollador en la plataforma de gestión de proyectos, tiene como función principal, ir rellenando el cumplimiento de controles en el checklist de los proyectos, indicando si se adhieren o no y por qué. Mientras tanto, en la plataforma del plan de concientización su único rol y función principal es realizar

las diversas pruebas disponibles. Por tanto, en la plataforma de gestión de proyectos sus funciones son:

- Visualizar proyectos y métricas asociados a este.
- Visualizar el checklist de controles asociados a los diversos proyectos.
- Modificar adherencia de un control en un proyecto, indicando por qué la adherencia o no a ese control.

Para la plataforma del plan de concientización las funciones que puede realizar son:

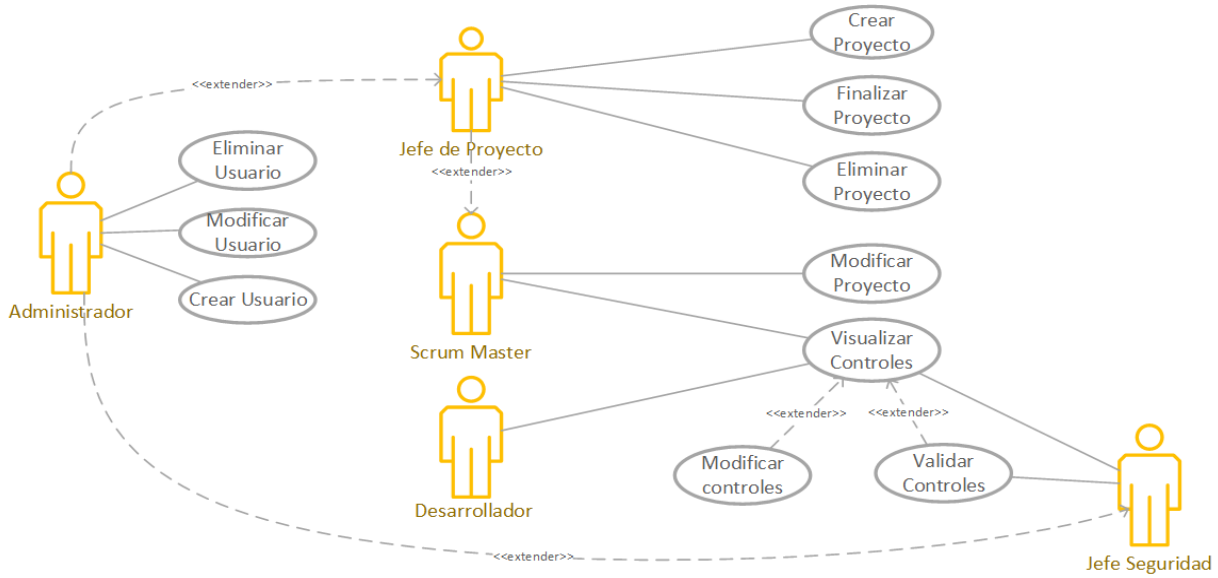
- Realizar Pruebas.
- Visualizar perfil personal, con métricas asociadas al desempeño en las diversas pruebas.

Cabe destacar que la concientización se debe realizar especialmente para el equipo de trabajo, incluyendo tanto desarrolladores, como jefe de proyecto, scrum master y auditor.

5.2 Análisis

5.2.1 Diagrama de casos de uso

Figura 10 – Diagrama caso de uso "Plataforma Metodología"



Fuente: Elaboración Propia

Como se puede visualizar en la figura 10, se tienen 5 actores, de los cuales el administrador es el encargado exclusivo de administrar los usuarios, además de ser capaz de realizar las funciones de todos los demás actores. Así también, el jefe de proyecto es el encargado de administrar los proyectos, junto con visualizar y modificar controles, los cuales son validados exclusivamente por el Jefe de Seguridad (posterior a su revisión). Finalmente, el Scrum Master puede modificar alguna información del proyecto, tal como el estado en que se encuentra el proyecto y la descripción, así también al igual que el Desarrollador, son capaces de visualizar los controles y modificar información de estos, como si se está adhiriendo determinado control, como también fundamentar el por qué se toma esa decisión.

Figura 11 – Diagrama caso de uso “Plataforma Concientización”

Fuente: Elaboración Propia

Como se puede visualizar en la figura anterior, se puede visualizar 5 actores, de los cuales el Administrador nuevamente es capaz de realizar todas las tareas (tanto administrar pruebas como realizarlas), mientras que el jefe de seguridad igualmente es el encargado de administrar las pruebas, y los demás actores como desarrollador, scrum master y jefe de proyecto son los que deben realizar las pruebas, para ser evaluados y “concientizados”.

A continuación, se describirá en extensión cada caso de uso con los casos extendidos.

Tabla 4 – Caso de uso extendido "Crear usuario"

Caso de Uso	Crear usuario
Actor	Administrador
Propósito	Añadir un usuario nuevo a la plataforma web.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de "Administración de usuarios", para así finalmente seleccionar crear usuario, rellenar la información respectiva y presionar el botón guardar para almacenar el usuario en la base de datos.
Escenario Principal	
Acción del Actor	**Respuesta del Sistema**
1. El usuario entra al sistema y selecciona la pestaña "Administración de usuarios".	
	2. El sistema despliega una lista de usuarios y las opciones disponibles a realizar en esa pestaña.
3. El usuario selecciona la opción de crear usuario.	4. El sistema despliega campos a ser rellenados por el usuario.
5. El usuario ingresa la información solicitada y presiona guardar para crear el nuevo usuario.	6. El sistema almacena el usuario correctamente.
Flujos Alternativos	5.1. En caso de ingresar algún valor incorrecto, se solicitará ingresar la información nuevamente.

Fuente: Elaboración Propia

Tabla 5 – Caso de uso extendido "Modificar usuario"

Caso de Uso	Modificar usuario
Actor	Administrador
Propósito	Modificar la información de un usuario de la plataforma web.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de "Administración de usuarios", después selecciona un usuario y presiona "Ver usuario", para finalmente seleccionar modificar usuario, modificar la información respectiva y guardar los cambios.

Escenario Principal	
Acción del Actor	**Respuesta del Sistema**
1. El usuario entra al sistema y selecciona la pestaña "Administración de usuarios".	
	2. El sistema despliega una lista de usuarios y las opciones disponibles a realizar en esa pestaña.
3. El usuario selecciona un usuario y presiona "Ver usuario".	4. El sistema despliega información de usuario y opciones a realizar.
5. El usuario selecciona "Modificar información usuario".	6. El sistema despliega los campos modificables del usuario.
7. El usuario ingresa la información a modificar y presiona el botón guardar.	8. El sistema almacena los cambios en la base de datos.
Flujos Alternativos	7.1. En caso de ingresar algún valor incorrecto, se solicitará ingresar la información nuevamente.

Fuente: Elaboración Propia

Tabla 6 – Caso de uso extendido “Eliminar usuario”

Caso de Uso	Eliminar usuario
Actor	Administrador
Propósito	Eliminar el acceso de un usuario en la plataforma web.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de “Administración de usuarios”, después selecciona un usuario y presiona “Ver usuario”, para finalmente seleccionar eliminar usuario.

Escenario Principal

Acción del Actor	Respuesta del Sistema
1. El usuario entra al sistema y selecciona la pestaña “Administración de usuarios”.	
	2. El sistema despliega una lista de usuarios y las opciones disponibles a realizar en esa pestaña.
3. El usuario selecciona un usuario y presiona “Ver usuario”.	4. El sistema despliega información de usuario y opciones a realizar.
5. El usuario selecciona “Eliminar usuario”.	6. El sistema elimina al usuario seleccionado de la base de datos.

Fuente: Elaboración Propia

Tabla 7 – Caso de uso extendido "Crear Proyecto"

Caso de Uso	Crear proyecto
Actor	Administrador, Jefe Proyecto
Propósito	Agregar un nuevo proyecto a la plataforma web para realizar seguimiento de los checklist de seguridad de la información.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de "Mis proyectos", después selecciona "Crear proyecto", para así finalmente rellenar la información solicitada y guardar así el proyecto.

Escenario Principal

Acción del Actor	Respuesta del Sistema
1. El usuario entra al sistema y selecciona la pestaña "Mis proyectos".	
	2. El sistema despliega la lista de proyectos disponibles y las opciones a realizar.
3. El usuario la opción presiona "Crear proyecto".	4. El sistema despliega los campos necesarios a rellenar para crear un proyecto.
5. El usuario rellena la información correspondiente y presiona el botón guardar	6. El sistema almacena el nuevo proyecto en la base de datos

Flujos Alternativos	5.1. En caso de ingresar algún valor incorrecto, se solicitará ingresar la información nuevamente.

Fuente: Elaboración Propia

Tabla 8 – Caso de uso extendido "Modificar proyecto"

Caso de Uso	Modificar proyecto
Actor	Administrador, Jefe Proyecto, Scrum Master
Propósito	Modificar la información respectiva de un proyecto ya existente, tal como la descripción de este o su estado.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de "Mis proyectos", después selecciona un proyecto y presiona "Ver proyecto", para así finalmente presionar modificar proyecto, rellenar la información a cambiar y guardar los cambios.

Escenario Principal

Acción del Actor	Respuesta del Sistema
1. El usuario entra al sistema y selecciona la pestaña "Mis proyectos".	
	2. El sistema despliega la lista de proyectos disponibles y las opciones a realizar.
3. El usuario selecciona un proyecto y presiona "Ver proyecto".	4. El sistema despliega la información del proyecto y las opciones a realizar.
5. El usuario selecciona la opción "Modificar proyecto".	6. El sistema despliega los campos a modificar del proyecto.
7. El usuario rellena la información a cambiar y presiona el botón guardar.	8. El sistema guarda los cambios realizados en la base de datos.
Flujos Alternativos	7.1. En caso de ingresar algún valor incorrecto, se solicitará ingresar la información nuevamente.

Fuente: Elaboración Propia

Tabla 9 – Caso de uso extendido - Finalizar Proyecto

Caso de Uso	Finalizar Proyecto
Actor	Administrador, Jefe Proyecto
Propósito	Finalizar un proyecto que se encuentre en estado de cierre del proyecto, con tal de que este no sea modificable y por tanto no sea accesible desde la plataforma, pero aun así se siga considerando como parte de las métricas generales.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de “Mis proyectos”, después selecciona un proyecto y presiona “Ver proyecto”, para así finalmente presionar en finalizar proyecto para cerrar este.

Escenario Principal

Acción del Actor	Respuesta del Sistema
1. El usuario entra al sistema y selecciona la pestaña “Mis proyectos”.	
	2. El sistema despliega la lista de proyectos disponibles y las opciones a realizar.
3. El usuario selecciona un proyecto y presiona “Ver proyecto”.	4. El sistema despliega la información del proyecto y las opciones a realizar.
5. El usuario selecciona la opción “Finalizar Proyecto”	6. El sistema cambia el estado del proyecto, dejándolo fuera de la plataforma, pero manteniéndolo como parte de las métricas generales de proyectos.

Fuente: Elaboración Propia

Tabla 10 – Caso de uso extendido "Eliminar proyecto"

Caso de Uso	Eliminar proyecto
Actor	Administrador, Jefe Proyecto
Propósito	Eliminar un proyecto de la plataforma web.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de "Mis proyectos", después selecciona un proyecto y presiona "Ver proyecto", para finalmente eliminar el proyecto seleccionado.

Escenario Principal	
Acción del Actor	**Respuesta del Sistema**
1. El usuario entra al sistema y selecciona la pestaña "Mis proyectos".	
	2. El sistema despliega una lista de proyectos activos y las opciones disponibles a realizar en esa pestaña.
3. El usuario selecciona un proyecto y presiona "Ver proyecto".	4. El sistema despliega información de proyecto y opciones a realizar.
5. El usuario selecciona "Eliminar proyecto".	6. El sistema elimina al proyecto seleccionado de la base de datos.

Fuente: Elaboración Propia

Tabla 11 – Caso de uso extendido "Visualizar Controles"

Caso de Uso	Visualizar Controles
Actor	Administrador, Jefe Proyecto, Scrum Master, Desarrollador, Jefe Seguridad, Auditor
Propósito	Visualizar la adherencia de controles de un proyecto.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de "Mis proyectos", después selecciona un proyecto y presiona "Ver proyecto", para finalmente visualizar los controles de determinado proyecto.

Escenario Principal

Acción del Actor	**Respuesta del Sistema**
1. El usuario entra al sistema y selecciona la pestaña "Mis proyectos".	
	2. El sistema despliega una lista de proyectos activos y las opciones disponibles a realizar en esa pestaña.
3. El usuario selecciona un proyecto y presiona "Ver proyecto".	4. El sistema despliega información de proyecto y opciones a realizar.
5. El usuario selecciona "Visualizar controles".	6. El sistema despliega los controles junto con la información respectiva (de adherencia) para el proyecto seleccionado.

Fuente: Elaboración Propia

Tabla 12 – Caso de uso extendido "Modificar controles"

Caso de Uso	Modificar Controles
Actor	Administrador, Jefe Proyecto, Scrum Master, Desarrollador
Propósito	Modificar información respecto a la adherencia de los controles del proyecto seleccionado.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de "Mis proyectos", después selecciona un proyecto y presiona "Ver proyecto", para finalmente visualizar los controles de determinado proyecto y tener acceso a modificar información respecto a su adherencia.

Escenario Principal

Acción del Actor	Respuesta del Sistema
1. El usuario entra al sistema y selecciona la pestaña "Mis proyectos".	
	2. El sistema despliega una lista de proyectos activos y las opciones disponibles a realizar en esa pestaña.
3. El usuario selecciona un proyecto y presiona "Ver proyecto".	4. El sistema despliega información de proyecto y opciones a realizar.
5. El usuario selecciona "Visualizar controles".	6. El sistema despliega los controles junto con la información respectiva (de adherencia) para el proyecto seleccionado y los posibles campos a modificar.
7. El usuario rellena los campos a modificar y presiona el botón guardar.	8. El sistema guarda los cambios realizados en la base de datos.

Fuente: Elaboración Propia

Tabla 13 – Caso de uso extendido "Validar controles"

Caso de Uso	Validar controles
Actor	Jefe de Seguridad
Propósito	Validar un control de un proyecto, de acuerdo con la información ingresada por el grupo de trabajo.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de "Mis proyectos", después selecciona un proyecto y presiona "Ver proyecto", para finalmente visualizar los controles de determinado proyecto y seleccionar validar un control.

Escenario Principal

Acción del Actor	Respuesta del Sistema
1. El usuario entra al sistema y selecciona la pestaña "Mis proyectos".	
	2. El sistema despliega una lista de proyectos activos y las opciones disponibles a realizar en esa pestaña.
3. El usuario selecciona un proyecto y presiona "Ver proyecto".	4. El sistema despliega información de proyecto y opciones a realizar.
5. El usuario selecciona "Visualizar controles".	6. El sistema despliega los controles junto con la información respectiva (de adherencia) para el proyecto seleccionado y los posibles campos a modificar.
7. El usuario presiona el botón validar control, para cambiar el estado de determinado control.	8. El sistema guarda los cambios realizados en la base de datos.

Fuente: Elaboración Propia

Tabla 14 – Caso de uso extendido "Crear Prueba"

Caso de Uso	Crear Prueba
Actor	Jefe de Seguridad, Administrador
Propósito	Crear una prueba para evaluar un tema de concientización a los usuarios.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de "Gestión de Pruebas", después selecciona la opción crear prueba, para finalmente rellenas los campos solicitados y así guardar la prueba.

Escenario Principal

Acción del Actor	Respuesta del Sistema
1. El usuario entra al sistema y selecciona la pestaña "Gestión de Pruebas".	
	2. El sistema despliega una lista de pruebas creadas y las opciones disponibles a realizar
3. El usuario selecciona la opción "Crear prueba".	4. El sistema despliega los campos a rellenar para la creación de la prueba.
5. El usuario rellena la información solicitada y presiona el botón guardar.	6. El sistema almacena la prueba en la base de datos.

Fuente: Elaboración Propia

Tabla 15 – Caso de uso extendido “Crear nueva prueba”

Caso de Uso	Crear nueva prueba
Actor	Jefe de Seguridad, Administrador
Propósito	Crear una prueba nueva con una categoría distinta a las ya predeterminadas en la plataforma para evaluar un tema de concientización a los usuarios.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de “Gestión de Pruebas”, después selecciona la opción crear prueba, donde seleccionará la opción crear nueva prueba, para así rellenas los campos solicitados y así guardar la prueba y la categoría nueva.

Escenario Principal

Acción del Actor	**Respuesta del Sistema**
1. El usuario entra al sistema y selecciona la pestaña “Gestión de Pruebas”.	
	2. El sistema despliega una lista de pruebas creadas y las opciones disponibles a realizar
3. El usuario selecciona la opción “Crear nueva prueba”.	4. El sistema despliega los campos a rellenar para la creación de la prueba.
5. El usuario rellena la información solicitada y presiona el botón guardar.	6. El sistema almacena la prueba en la base de datos.

Fuente: Elaboración Propia

Tabla 16 – Caso de uso extendido “Previsualizar video”

Caso de Uso	Previsualizar video
Actor	Jefe de Seguridad, Administrador
Propósito	Previsualizar el video de la categoría de la prueba a crear.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de “Gestión de Pruebas”, después selecciona la opción crear prueba, donde seleccionará la opción previsualizar video para así ver si el video es acorde a las necesidades sugeridas por el Jefe de Seguridad.

Escenario Principal	
Acción del Actor	**Respuesta del Sistema**
1. El usuario entra al sistema y selecciona la pestaña “Gestión de Pruebas”.	
	2. El sistema despliega una lista de pruebas creadas y las opciones disponibles a realizar
3. El usuario selecciona la opción “Crear prueba”.	4. El sistema despliega los campos a rellenar y acciones a realizar
5. El usuario selecciona una categoría y oprime “Previsualizar video”	6. El sistema despliega una ventana con el video asociado a esa categoría

Fuente: Elaboración Propia

Tabla 17 – Caso de uso extendido “Eliminar prueba”

Caso de Uso	Eliminar prueba
Actor	Jefe de Seguridad, Administrador
Propósito	Eliminar prueba activa de concientización de la plataforma web.
Resumen	El usuario entra al sistema, luego selecciona la pestaña de “Gestión de Pruebas”, después selecciona una prueba y oprime “Ver prueba”, para así seleccionar la opción de eliminar la prueba seleccionada.

Escenario Principal	
Acción del Actor	**Respuesta del Sistema**
1. El usuario entra al sistema y selecciona la pestaña “Gestión de Pruebas”.	
	2. El sistema despliega una lista de pruebas creadas y las opciones disponibles a realizar
3. El usuario selecciona una prueba y oprime “Ver prueba”.	4. El sistema la información de la prueba y las acciones a realizar.
5. El usuario oprime “Eliminar prueba”.	6. El sistema elimina la prueba de la base de datos.

Fuente: Elaboración Propia

Tabla 18 – Caso de uso extendido “Realizar prueba”

Caso de Uso	Realizar prueba
Actor	Jefe proyecto, Scrum Master, Desarrollador
Propósito	Realizar y responder las preguntas de las pruebas de concientización agendadas para evaluar las concientizaciones realizadas de manera presencial para el grupo de trabajo.
Resumen	El usuario entra al sistema, luego en la pestaña de inicio selecciona una prueba activa, para luego seleccionar el botón “Realizar prueba” y comenzar la evaluación donde se seleccionarán las respuestas correspondientes y se guardarán finalmente los resultados.

Escenario Principal

Acción del Actor	Respuesta del Sistema
1. El usuario entra al sistema y en la pestaña inicial selecciona alguna prueba activa.	
	2. El sistema despliega una ventana con la previsualización del video previo a la prueba, además de la opción de comenzar la prueba.
3. El usuario oprime el botón “Realizar prueba”.	4. El sistema despliega las preguntas y las respuestas posibles.
5. El usuario selecciona las respuestas correctas y presiona finalizar.	6. El sistema guarda los resultados en la base de datos.

Fuente: Elaboración Propia

5.3 Diseño

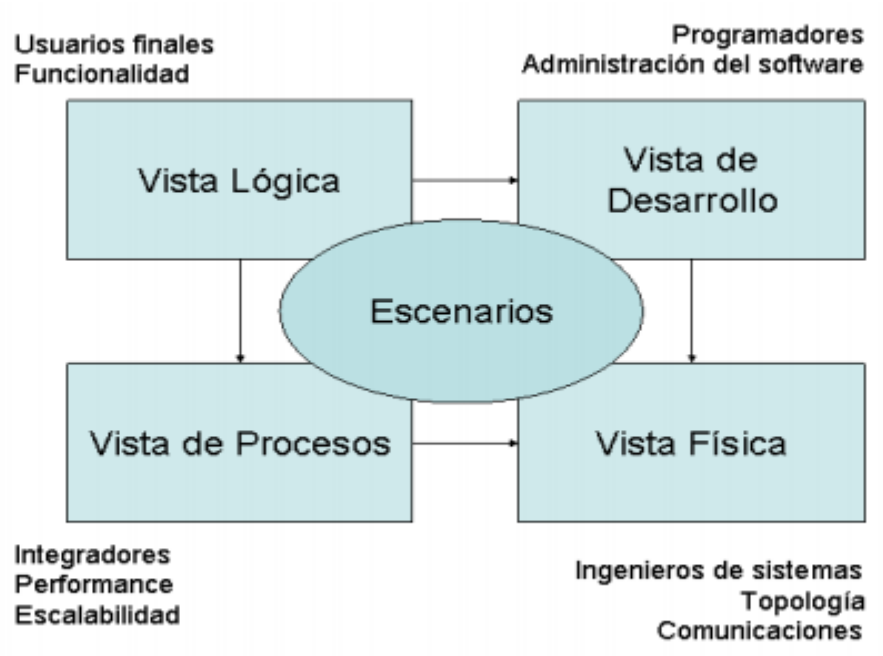
5.3.1 Modelo de vistas de arquitectura 4+1

Para el diseño del producto se aplicará el modelo de vistas de arquitectura 4+1 (4 vistas + 1), un modelo diseñado por el profesor Philippe Kruchten, el cual se utiliza para describir la arquitectura de un software desde distintos puntos de vistas (Kruchten, 1995), las cuales serán descritas a continuación:

- Vista lógica: Representa las funcionalidades que el sistema proporciona a los usuarios finales.
- Vista de desarrollo: Se visualiza el sistema desde el punto de vista de los programadores, y se basa en describir cómo se divide el software/sistema y las dependencias que hay entre estos componentes.
- Vista de procesos: Se representa desde la perspectiva de un integrador de sistema, en donde se visualiza los procesos existentes en el sistema y como se comunican entre sí.
- Vista física: Se representa desde la perspectiva de un ingeniero de sistemas, en donde se muestran las conexiones entre los diversos componentes físicos que integran el sistema.
- Vista de escenarios (+1): Se representa por los casos de uso (las funciones que pueden realizar los usuarios), la cual su función es unir las otras vistas teniendo una trazabilidad de componentes, clases, paquetes, etc., para realizar cada caso de uso.

A continuación, se podrá visualizar un diagrama de las distintas vistas del modelo 4+1.

Figura 12 – Modelo de vistas de arquitectura 4+1



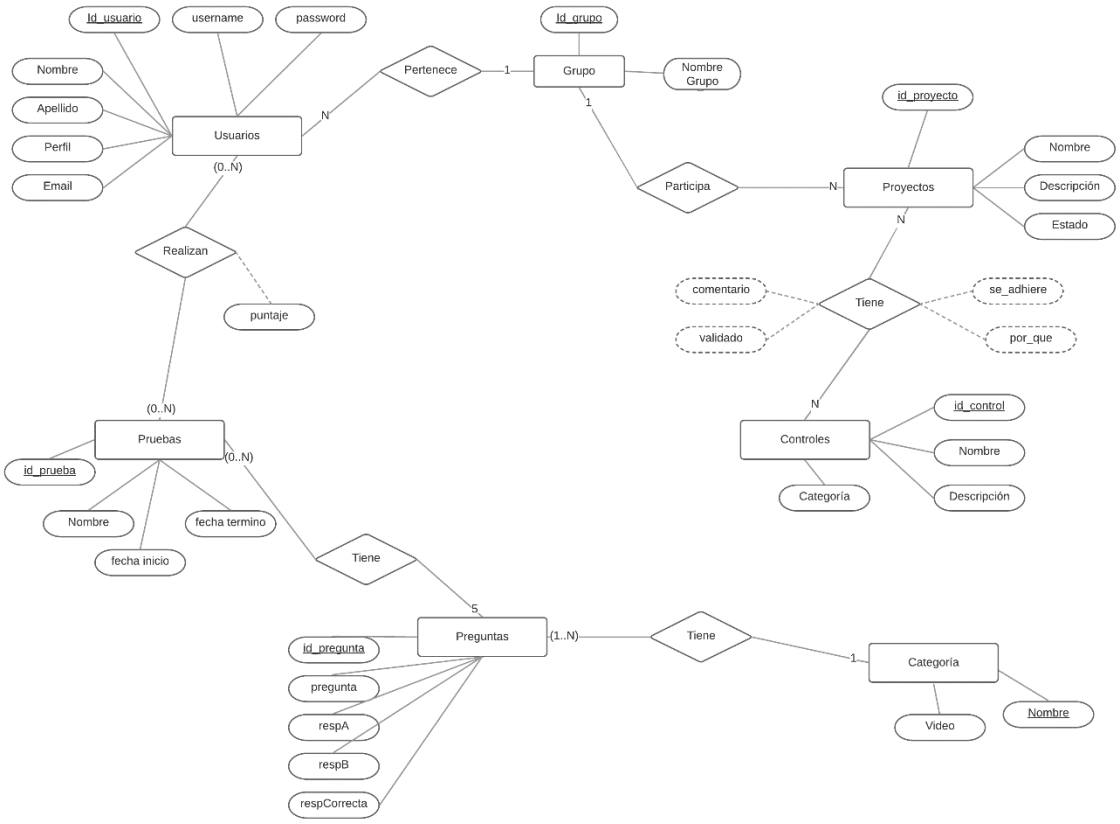
Fuente: (Kruchten, 1995)

Los diagramas y modelos para describir cada vista serán descritos a continuación:

- Vista Lógica:
  - Diagrama de Secuencia.
  - Diagrama entidad-relación.
  - Modelo relacional.
- Vista de Desarrollo:
  - Diagrama de paquetes.
- Vista de Procesos:
  - Diagrama de actividad.
- Vista Física:
  - Diagrama de despliegue.
- Escenarios:
  - Casos de uso.

5.3.2 Modelo Entidad – Relación

Figura 13 – Modelo Entidad – Relación (ER)



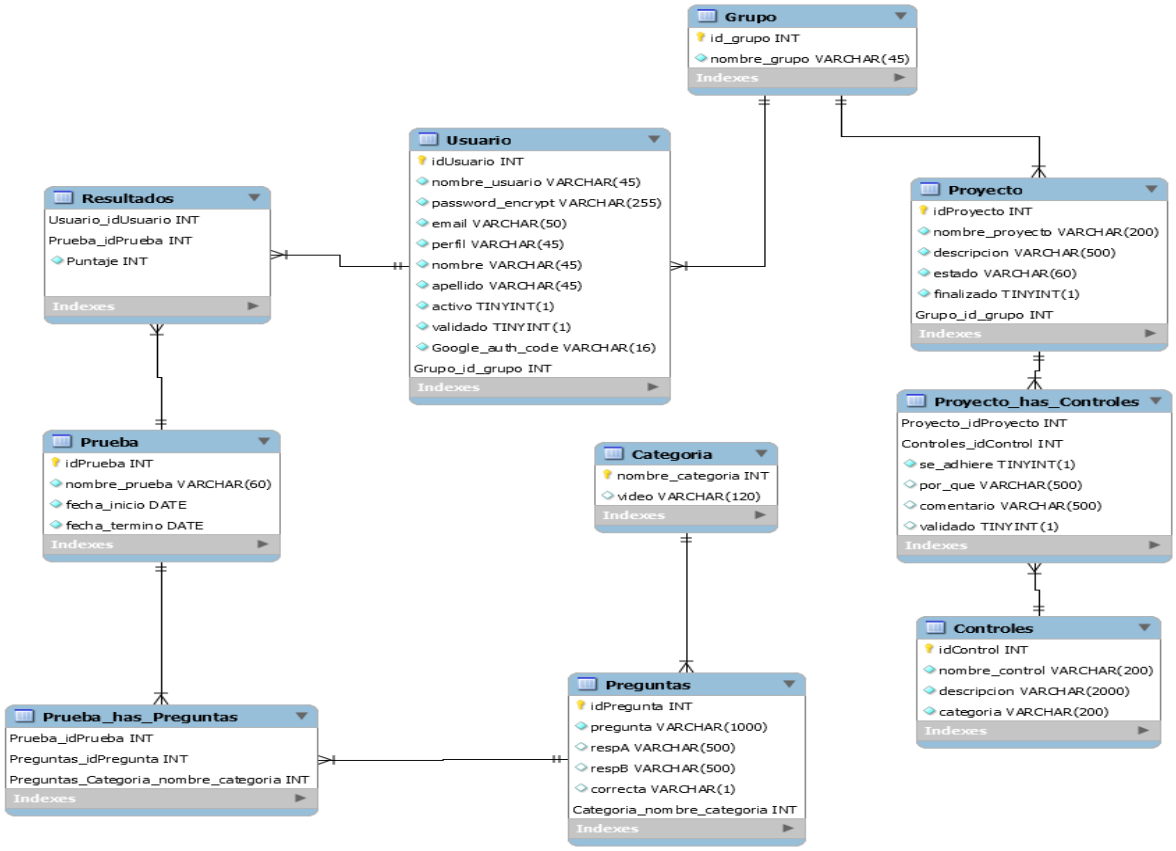
Fuente: Elaboración Propia

En la figura 13 se puede visualizar que hay 7 entidades: Usuarios, Grupos, Proyectos, Controles, Pruebas, Preguntas y Categoría. Según las relaciones se puede ver que un usuario pertenece a un grupo de trabajo, los que pueden participar en uno o muchos proyectos, pero en un proyecto puede participar solo un grupo de trabajo. A su vez, un proyecto puede tener muchos controles, mientras que un control puede estar asociado a uno o muchos proyectos. Por otra parte, los usuarios pueden realizar muchas pruebas de concientización, las que a su vez pueden ser realizadas por uno o más usuarios. Las pruebas poseen estrictamente cinco preguntas, las cuales a su vez pueden en una o más pruebas, ya que de las preguntas de determinada categoría se seleccionan preguntas al azar para ser asignadas a la prueba. Finalmente, las preguntas pertenecen

a una sola categoría de algún tema a concientizar (ya sea malware, phishing, etc.), pero lógicamente en cada categoría pueden existir muchas preguntas.

5.3.3 Modelo Relacional

Figura 14 – Modelo Relacional



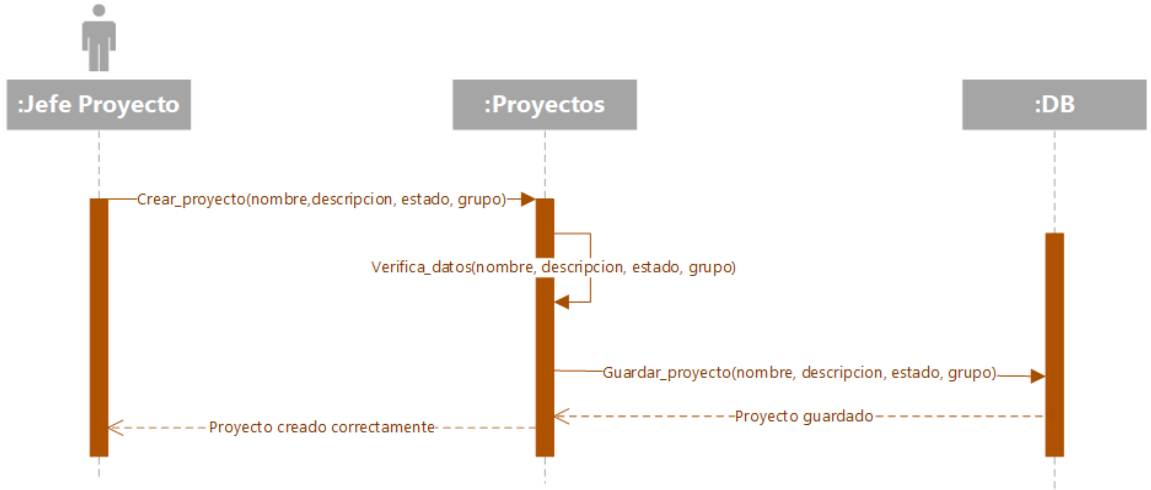
Fuente: Elaboración Propia

En la figura 14 se puede visualizar el esquema relacional de base de datos, en la cual se tienen 7 tablas principales: Usuario, Grupo, Proyecto, Controles, Prueba, Preguntas y Categoría. Al igual que en el modelo ER se tiene una relación uno a muchos entre usuarios y grupos, al igual que entre grupos y proyectos, además se tiene una relación muchos a muchos entre proyectos y controles, generando así una tabla adicional intermedia, la que almacena los controles por proyecto y su información al respecto (si

se adhiere, por qué, y si está validado por el jefe de seguridad). Por otra parte, existe una relación muchos a muchos entre usuario y prueba, generando otra tabla intermedia llamada “Resultados” la que almacena el resultado en determinada prueba de los diversos usuarios que rindieron la prueba. Finalmente, se tiene una relación 1 a muchos entre preguntas y categorías, ya que cada pregunta está asociada a una categoría en específica.

5.3.4 Diagramas de Secuencia

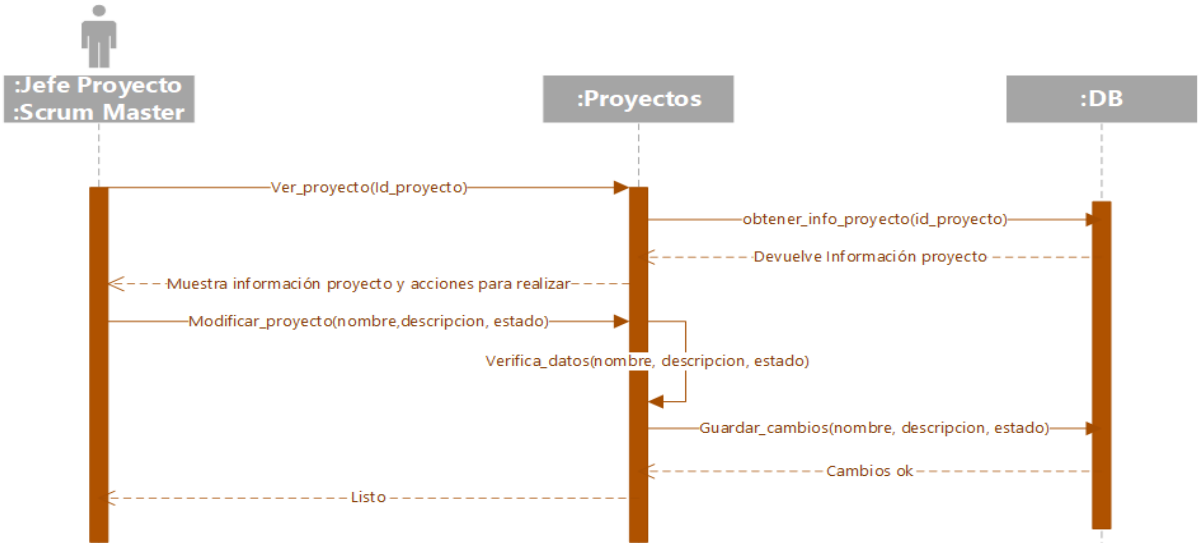
Figura 15 – Diagrama Secuencia – “Crear Proyecto”



Fuente: Elaboración Propia

En la figura anterior se puede visualizar el diagrama de secuencia para crear proyecto, en donde el Jefe de proyecto (o el administrador) una vez ingresado al sistema, solicita crear un proyecto, en el que ingresará su nombre, descripción, estado y grupo de trabajo a cargo del proyecto. Luego, se verifican los datos, para finalmente solicitar el guardado en la base de datos.

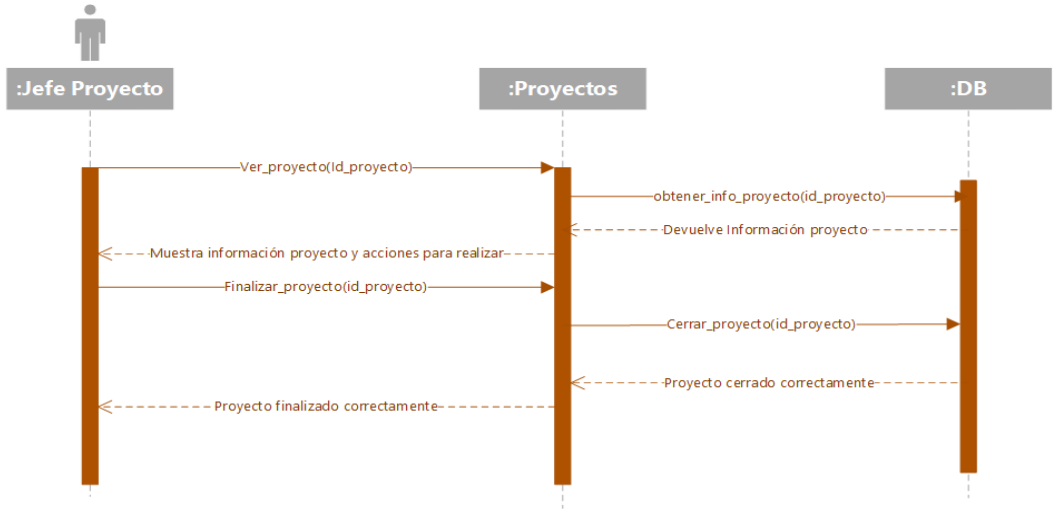
Figura 16 – Diagrama de secuencia "Modificar Proyecto"



Fuente: Elaboración Propia

En el diagrama de secuencia anterior, se puede ver que el jefe de proyecto, scrum master y administrador para modificar un proyecto, inicialmente, se solicita ver un proyecto, en el que luego se devuelve la información de este y las acciones a realizar, luego solicitan modificar proyecto, entregando así la información respectiva, luego se verifican los datos, y si están correctos se guardan los cambios en la base de datos. En el caso del administrador este será el único capaz de cambiar el grupo de trabajo a cargo del proyecto.

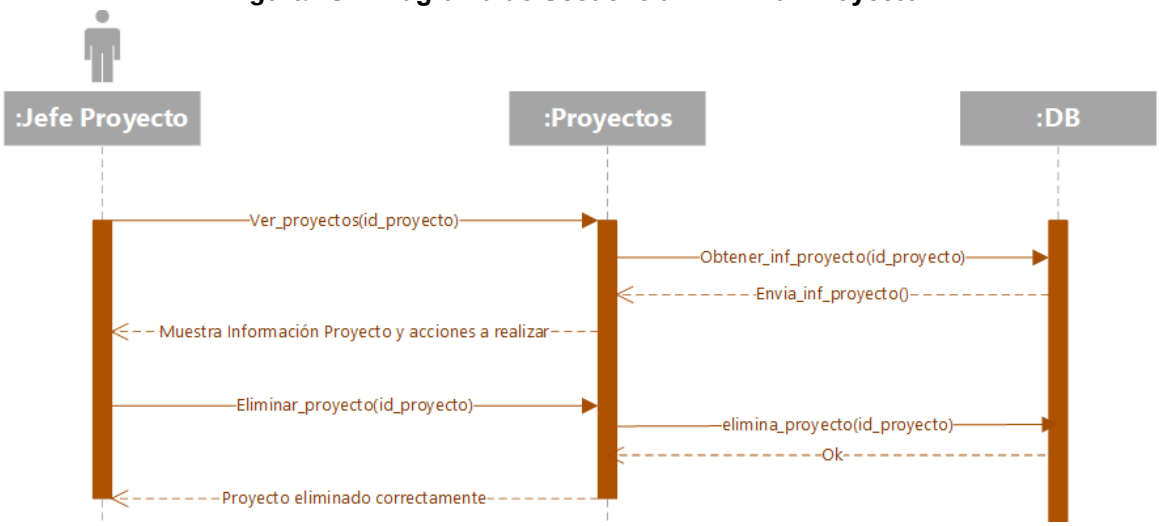
Figura 17 – Diagrama de secuencia "Finalizar Proyecto"



Fuente: Elaboración Propia

En la figura anterior, se puede visualizar la secuencia de pasos realizadas por el jefe de proyecto (o Administrador) para finalizar un proyecto. Para esto, el usuario solicita ver el proyecto a finalizar, donde se muestra la información y acciones a realizar, posteriormente, si y solo si el proyecto se encuentra en la etapa de Cierre, se entregará la opción de finalizar proyecto, donde una vez presionado el botón se realizará la finalización total de este, impidiendo de que se pueda modificar como también de aparecer directamente en la lista de proyectos actuales, sin embargo sus resultados no se borrarán como parte de las métricas de proyectos.

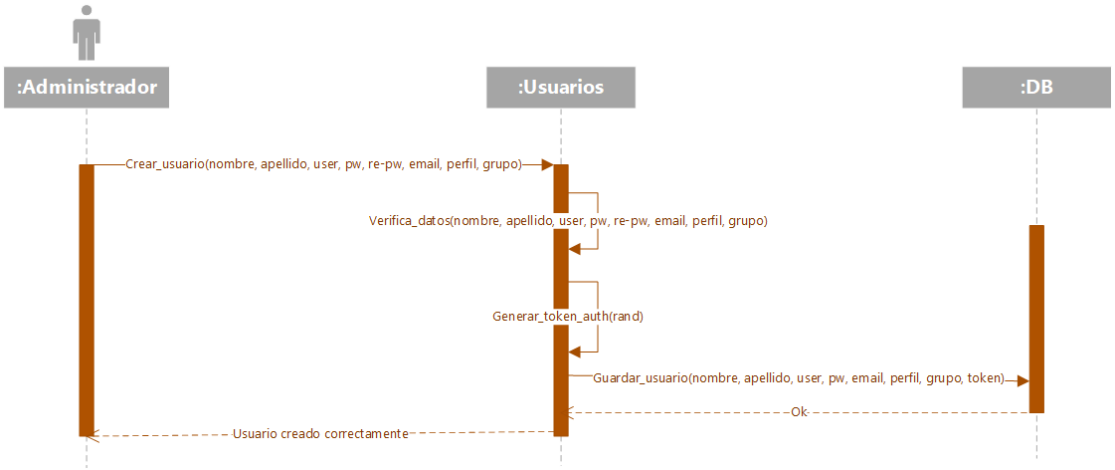
Figura 18 – Diagrama de Secuencia "Eliminar Proyecto"



Fuente: Elaboración Propia

En la figura anterior, se puede visualizar la secuencia para eliminar un proyecto, en la que inicia con el jefe de proyecto o administrador, solicitando ver un proyecto, en el que luego se obtiene la información de la base de datos, para ser mostrada junto con las acciones a realizar, para finalmente solicitar eliminar el proyecto seleccionado.

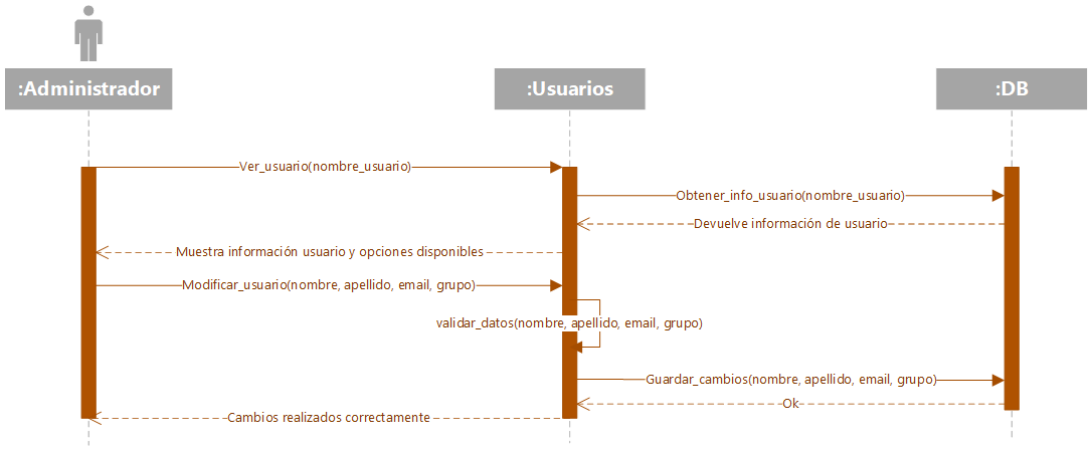
Figura 19 – Diagrama de Secuencia “Crear Usuario”



Fuente: Elaboración Propia

En la figura 19, se puede visualizar la secuencia de pasos para crear usuarios, en la que inicialmente el administrador solicita crear un usuario, en donde ingresa la información del usuario y el grupo de trabajo donde se integrará, luego se verifican los datos ingresados (como la contraseña que cumpla con la estructura solicitada), luego se genera un token de autorización para la generación de QR con el autenticador de Google, para finalmente guardar al usuario en la base de datos.

Figura 20 – Diagrama de Secuencia “Modificar Usuario”



Fuente: Elaboración Propia

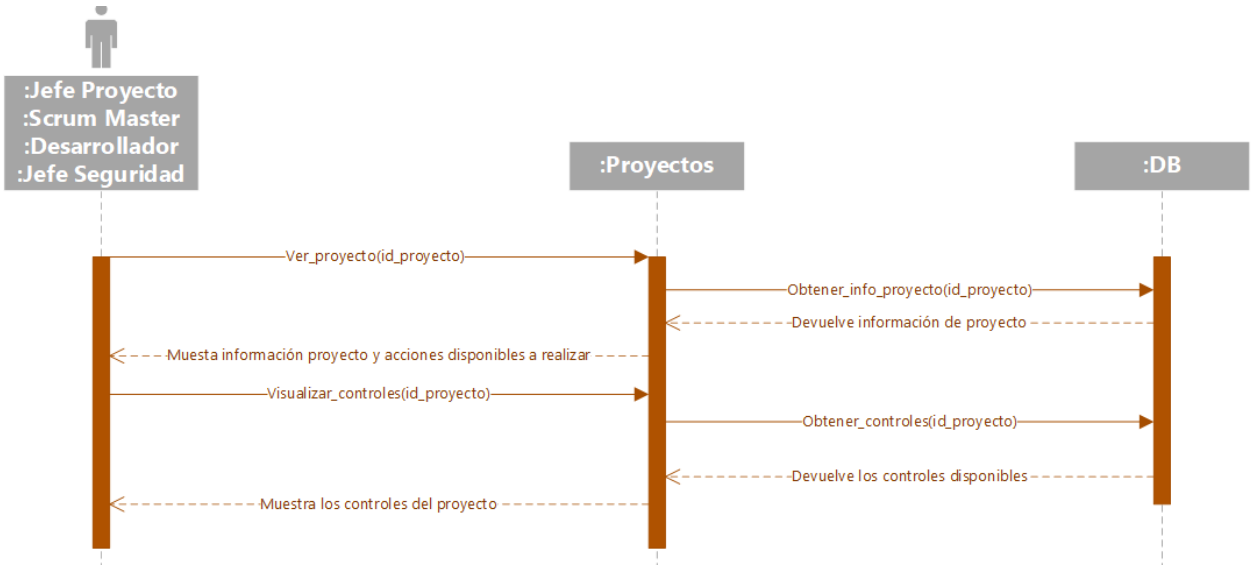
En la figura anterior, se puede visualizar la secuencia de pasos para modificar la información de un usuario, para esto, inicialmente el administrador solicita ver la información de un usuario, luego se obtiene la información del respectivo usuario en la base de datos y se muestra en pantalla junto con las opciones disponibles a realizar, posteriormente el administrador solicita modificar la información de este usuario indicando los valores a cambiar, para luego validarlos y finalmente guardar los cambios en la base de datos.

Figura 21 – Diagrama de Secuencia "Eliminar Usuario"

Fuente: Elaboración Propia

En la figura 21, se puede visualizar la secuencia de pasos para eliminar un usuario de la plataforma web. En este proceso, el administrador comienza solicitando ver la información de un usuario de la plataforma, donde se despliega la información de este y las acciones a realizar, posteriormente el usuario selecciona eliminar usuario para finalmente ser eliminado de la base de datos.

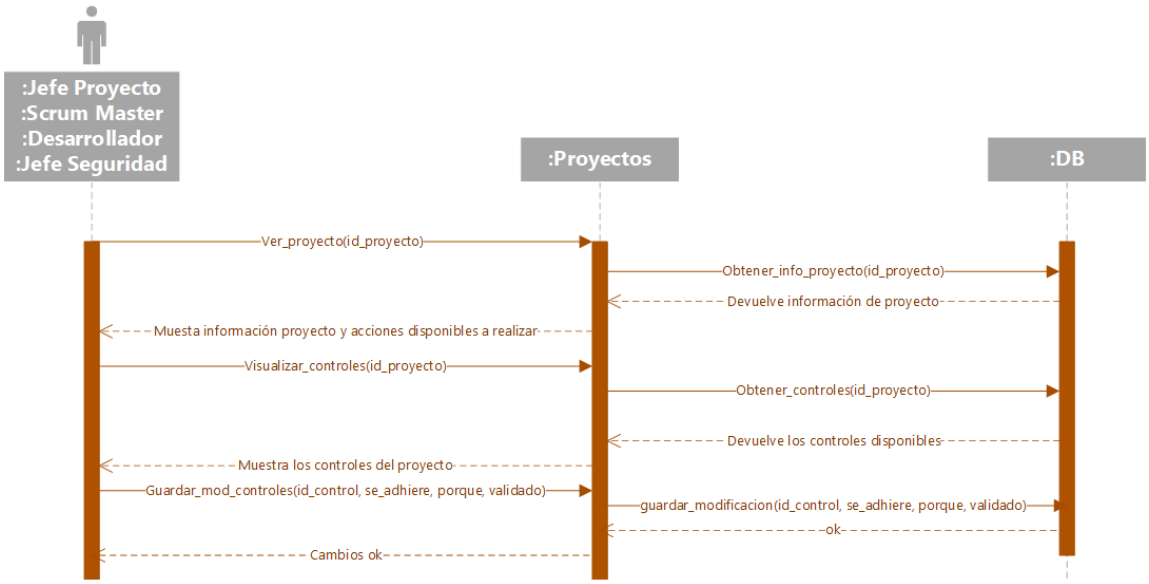
Figura 22 – Diagrama de Secuencia “Visualizar Controles”



Fuente: Elaboración Propia

En la figura 22, se puede visualizar la secuencia para visualizar los controles de los diversos proyectos. Inicialmente los usuarios solicitan ver un proyecto. Una vez obtenida la información del proyecto, se muestra junto con las acciones posibles a realizar. Posteriormente, se solicitar visualizar los controles de este proyecto, mostrando así finalmente los controles del proyecto.

Figura 23 – Diagrama de Secuencia “Modificar información controles”



Fuente: Elaboración Propia

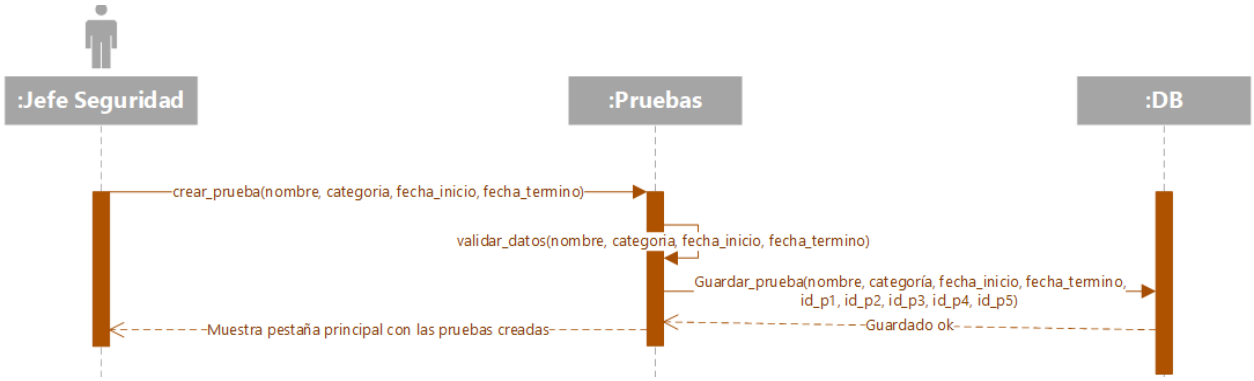
En la figura anterior se puede visualizar la secuencia para modificar la información de los controles de un proyecto. Inicialmente se solicita ver proyecto, luego se muestra la información obtenida en la base de datos, junto con las posibles acciones a realizar. Seguido a esto se solicita visualizar controles, de la cual se despliegan los controles del proyecto. Finalmente, el usuario solicita guardar las modificaciones correspondientes, enviando la información correspondiente de los controles.

Figura 24 – Diagrama de Secuencia "Validar control"

Fuente: Elaboración Propia

En la figura anterior se puede visualizar la secuencia para validar un control de determinado proyecto. Inicialmente, el usuario comienza solicitando ver un proyecto. Una vez mostrada la información se solicita visualizar los controles, los cuales son desplegados. Finalmente se solicita validar un control, para posteriormente guardar el estado de este.

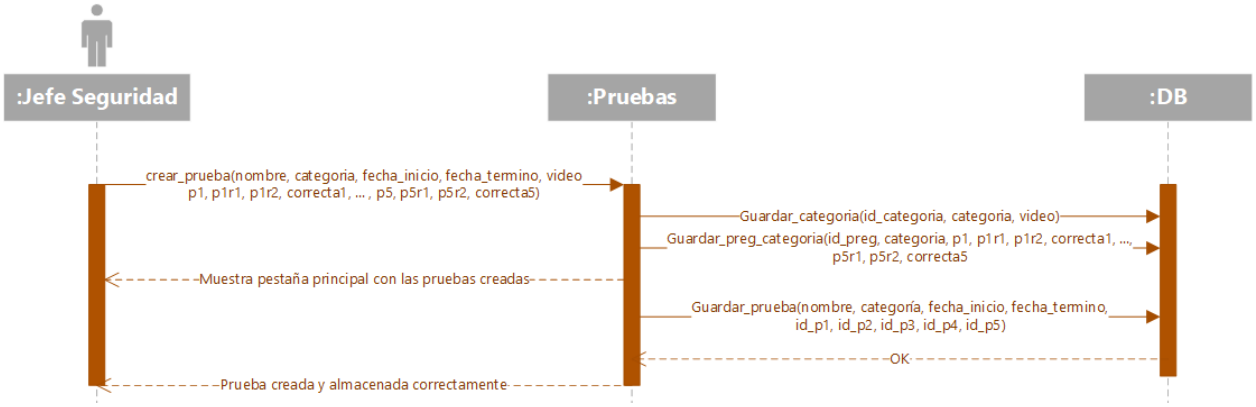
Figura 25 – Diagrama de Secuencia “Crear Prueba”



Fuente: Elaboración Propia

En la figura 25, se puede visualizar la secuencia para crear una prueba. En este caso el jefe de seguridad (o el administrador) solicitan crear una prueba, entregando los datos correspondientes. Finalmente, luego de validar los datos, se guarda la prueba en la base de datos, junto con las preguntas seleccionadas aleatoriamente a partir de la categoría elegida.

Figura 26 – Diagrama de Secuencia “Crear nueva prueba”

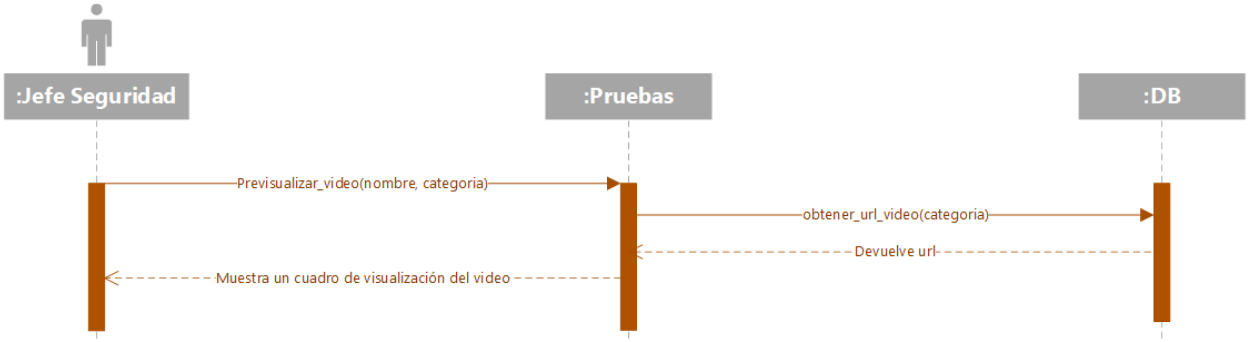


Fuente: Elaboración Propia

Como se puede visualizar en la figura 26, se describe la secuencia para crear una prueba nueva, la cual comienza el usuario solicitando crear una prueba nueva (con una nueva categoría) entregando los datos correspondientes a la prueba, como también los datos de la nueva categoría, tal como las preguntas, respuestas y link de video. Después

de validar los datos, se guarda la categoría nueva, se guardan las nuevas preguntas, para finalmente guardar la prueba.

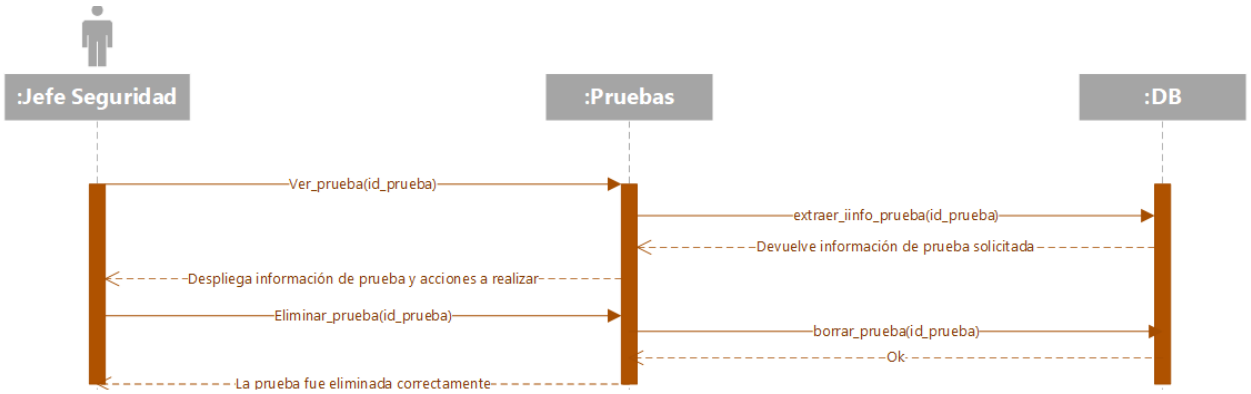
Figura 27 – Diagrama de Secuencia "Previsualizar video"



Fuente: Elaboración Propia

En la figura 27, se puede ver la secuencia de pasos para previsualizar el video de la prueba a crear. Inicialmente, el usuario solicita previsualizar video, para luego obtener la url y finalmente mostrar un cuadro de visualización del video.

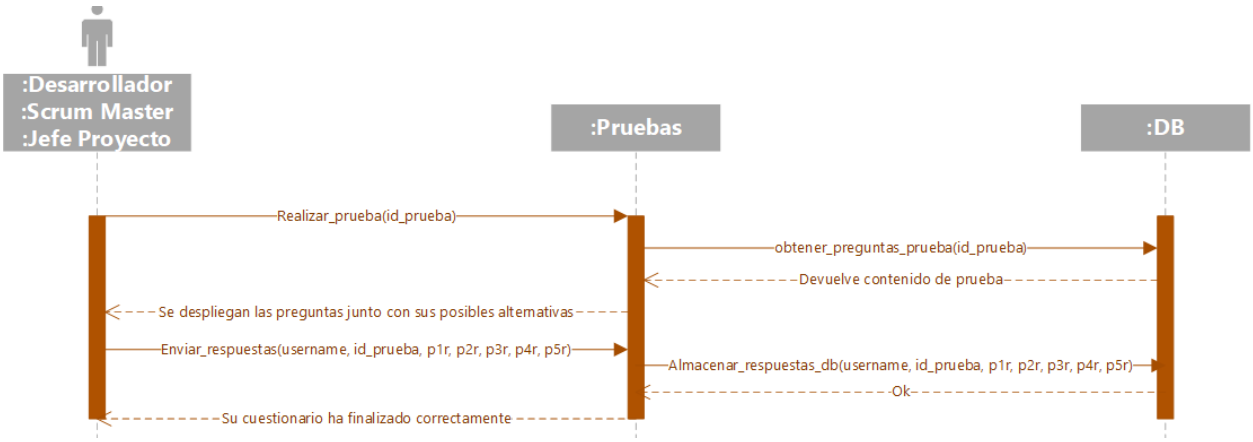
Figura 28 – Diagrama de Secuencia "Eliminar Prueba"



Fuente: Elaboración Propia

En la figura 28, se puede visualizar la secuencia para eliminar una prueba, para esto el usuario inicialmente solicita ver la prueba a eliminar, una vez obtenida la información se despliega junto con las acciones a realizar, para finalmente solicitar la eliminación de la prueba seleccionada de la base de datos.

Figura 29 – Diagrama de Secuencia “Realizar Prueba”

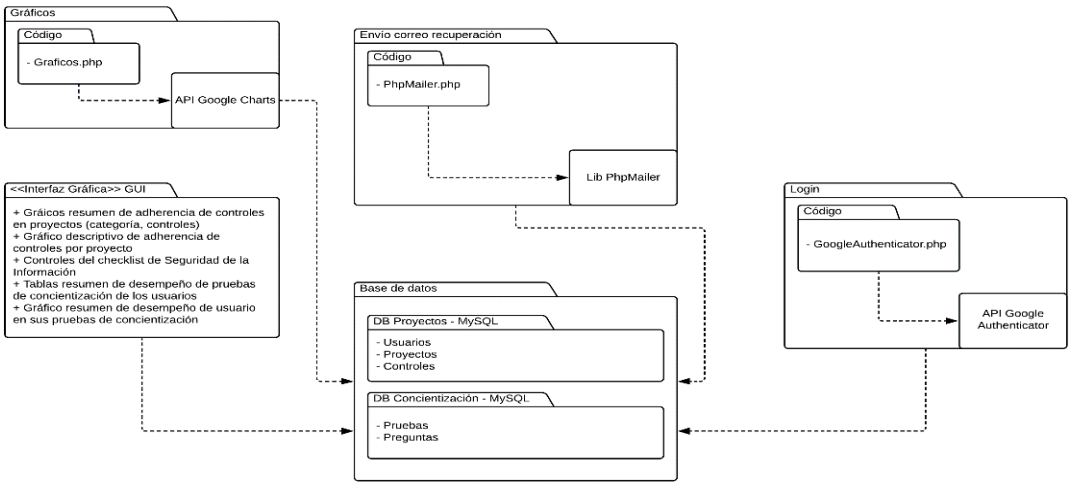


Fuente: Elaboración Propia

En la figura 29, se puede visualizar la secuencia de pasos para realizar una prueba. En este caso, los usuarios solicitan realizar una prueba, luego se obtiene las preguntas de la base de datos, para ser desplegadas. Finalmente, se envían las respuestas correspondientes de cada pregunta, para ser almacenados en la base de datos y así finalizar el cuestionario.

5.3.5 Diagrama de Paquetes

Figura 30 – Diagrama de paquetes

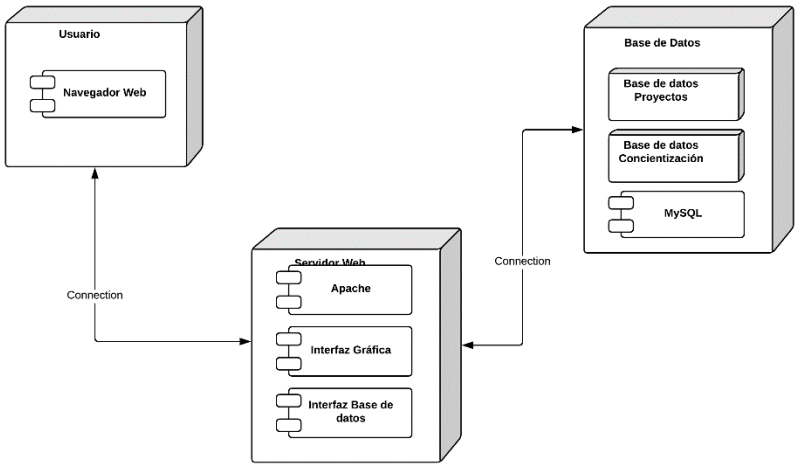


Fuente: Elaboración Propia

En la figura anterior, se puede visualizar como se descompone cada paquete que compone la plataforma web. En este caso se puede ver que el paquete de login, el cual utiliza la API de Google Authenticator, se encarga de generar y almacenar el token de autenticación de los usuarios, con tal de quedar enrolado con la aplicación móvil del autenticador. Asimismo, el paquete de correo de recuperación junto con la librería PhpMailer permite realizar cambios en la contraseña de los usuarios, actualizando así la contraseña en la base de datos. Finalmente, el paquete de gráficos, junto con la API de Google Charts permite crear gráficos descriptivos de la información almacenada en la base de datos.

5.3.6 Diagrama de Despliegue

Figura 31 – Diagrama de Despliegue



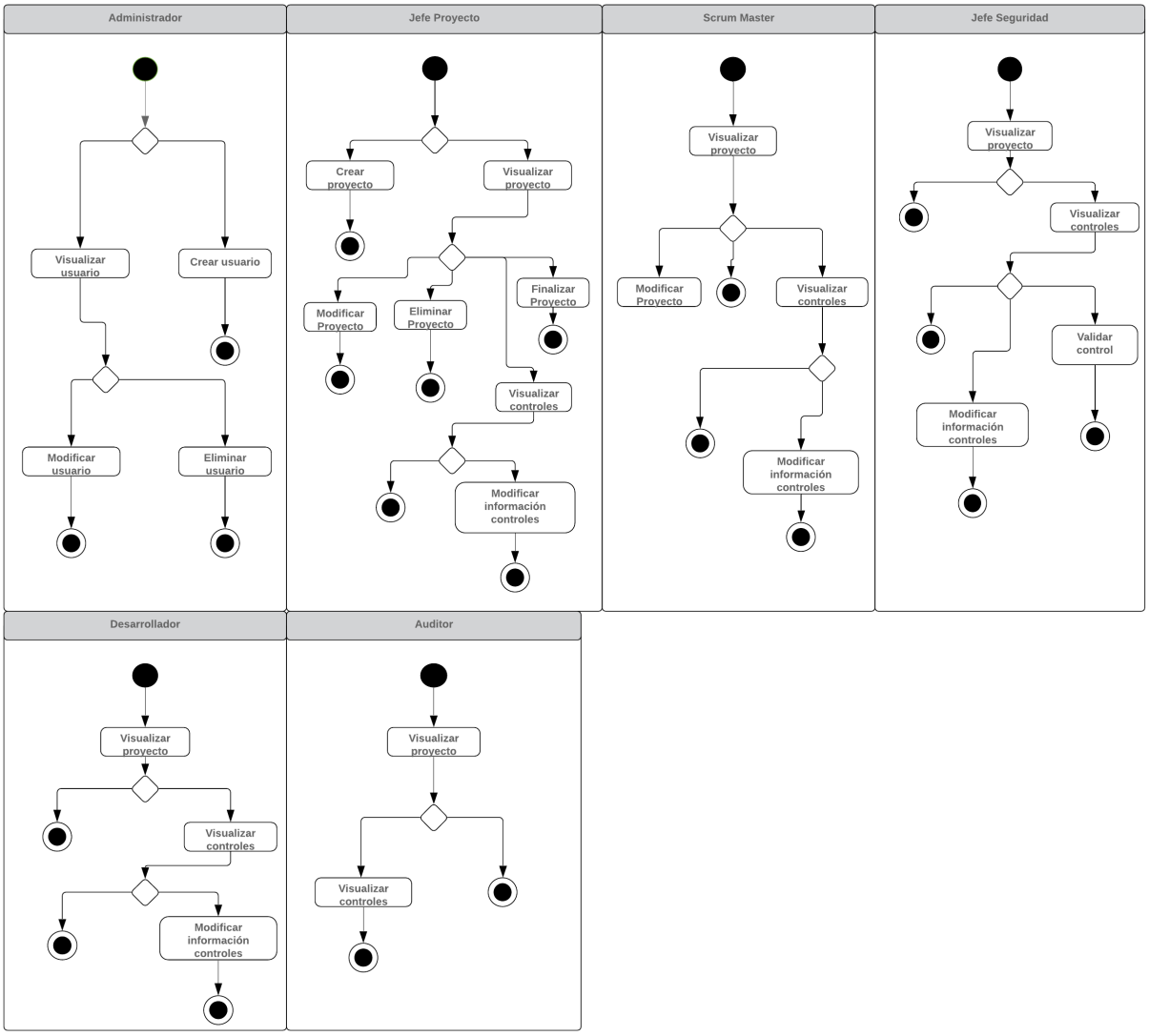
Fuente: Elaboración Propia

En la figura 31, se modela la topología del hardware sobre el cual se ejecuta el sistema. En esta plataforma web, se tienen 3 nodos: Usuario (cliente), Servidor Web y Base de Datos, dejando en claro una arquitectura Cliente – Servidor, donde el usuario, mediante un navegador web, ingresa a la plataforma, en la cual se mostrará una interfaz

gráfica y con una interfaz de base de datos, la que interactuará con la base de datos MySQL realizando las solicitudes y recibiendo los resultados de estas de manera interna.

5.3.7 Diagrama de Actividades

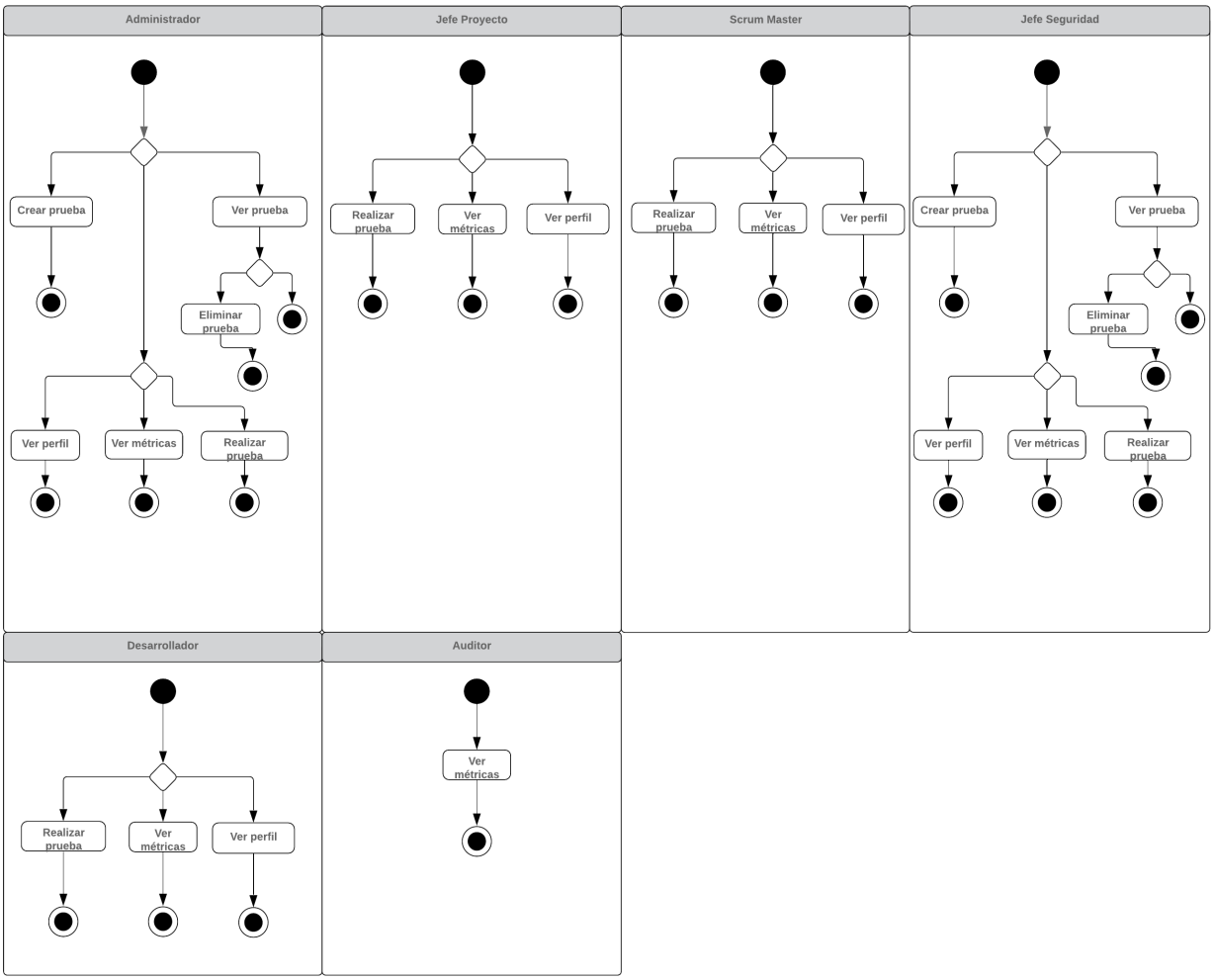
Figura 32 – Diagrama de Actividades Plataforma Metodología



Fuente: Elaboración propia

En la figura anterior se puede visualizar el diagrama de actividad para cada actor en el sistema. En este se puede visualizar la relación entre las actividades que pueden realizar estos actores en la plataforma de metodología, en las cuales las principales tareas a realizar se basan en gestión de usuarios, gestión de proyectos, visualización de usuarios, proyectos y controles, como también de también modificación de estos y validación de controles (según el perfil del usuario).

Figura 33 – Diagrama de Actividades Plataforma Concientización



Fuente: Elaboración Propia

En la figura anterior se puede visualizar el diagrama de actividad para cada actor en el sistema. En este se puede visualizar la relación entre las actividades que pueden realizar estos actores en la plataforma de concientización, en las cuales las principales tareas a realizar se basan en gestión de pruebas (crear o eliminar pruebas, ya sea de una categoría predeterminada o añadir otra), y visualización de métricas, tanto a nivel general como de usuario.

5.3.8 Front-End

El diseño de la página web se realizó de manera que sea fácil de utilizar para los usuarios, teniendo solo las funciones justas y necesarias para cada perfil. En el anexo A5 se podrán visualizar imágenes del diseño final de la plataforma web.

CAPÍTULO VI – ANÁLISIS DE RESULTADOS Y CONCLUSIONES

En este capítulo se abordará los resultados y el análisis respectivos en el ambiente donde se probó la propuesta dada en este documento. La propuesta fue testeada en el área de Seguridad de la Información en el Banco Itaú, sin embargo, dado que el banco está bajo el cumplimiento de diversas normas y de la SBIF (Superintendencia de Bancos e Instituciones Financieras), es que al comienzo de cada proyecto (pre-proyecto) se evaluó el checklist original del banco, ya que se poseen varios checklist distintos según la solución propuesta:

- Checklist para Proyectos Tradicionales
- Checklist para Proyectos Cloud
- Checklist para Proyectos que incluya Proveedores
- Checklist Proyecto Tradicional + Cloud
- Checklist Proyecto Tradicional + Proveedores
- Checklist Proyecto Cloud + Proveedores

Una vez aprobada la solución propuesta y comenzando el proyecto como tal, comienza la aplicación de la metodología, en donde el checklist propuesto se utilizó como filtro en la aprobación de cada proyecto durante las comisiones.

La propuesta fue aplicada durante un periodo de 3 meses (Enero hasta mediados de Marzo aproximadamente), por lo que es importante mencionar que los resultados pueden no ser representativos, debido a las distintas validaciones y/o comunicación que debe pasar un proyecto previamente para avanzar a la siguiente etapa de desarrollo. Por esta razón, y dado la metodología de trabajo del banco para el desarrollo de proyectos, se evaluó el cumplimiento del checklist y la cantidad de vulnerabilidades encontradas según las reuniones que se realizaban para certificar y validar el proyecto en sus distintas etapas antes de seguir avanzando.

6.1 Resultados Previos

Para los resultados previos se consideró los proyectos pasados por las comisiones durante el año 2018. Durante este año, se presentaron 148 proyectos en las comisiones (se incluyen los proyectos que se presentaron más de una vez, ya sea por ser rechazados o presentando una etapa distinta del proyecto), de los cuales en total se identificaron 30 riesgos totales. De estos riesgos, 14 fueron mitigados (correspondiente al 46%), mientras 16 no lo fueron (correspondiente a un 54%). En la tabla a continuación se podrá visualizar la distribución de los riesgos según su criticidad.

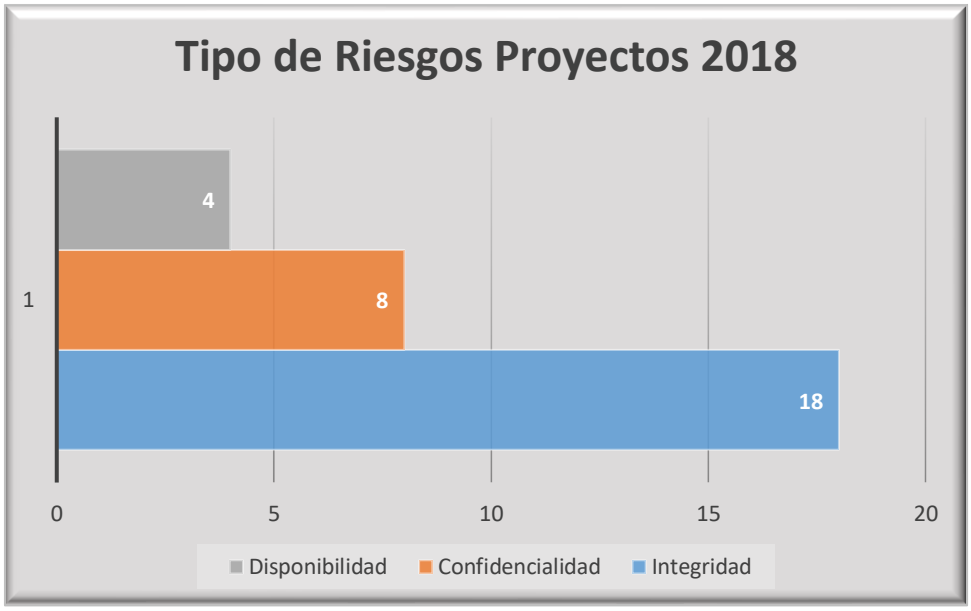
Tabla 19 - Riegos proyectos 2018 según su criticidad

Criticidad Riesgo	Cantidad
Crítico	3
Elevado	18
Moderado	9
Bajo	0

Fuente: Elaboración Propia

Como se puede ver durante el año 2018 en los proyectos presentados a las comisiones, existe un gran nivel de riesgos elevados, aun así, existen 3 riesgos críticos lo que igualmente es preocupante al momento de desarrollar un proyecto. Además, del total de estos riesgos, solo un 46% de estos riesgos fueron mitigados (desde la fecha en que fue encontrado este riesgo hasta febrero del 2019, periodo en que se realizó una validación de estos), lo cual lógicamente es muy preocupante que más de la mitad de los riesgos aún no fuesen mitigados. Así también, la distribución de los riesgos según el tipo de riesgo (basado en Disponibilidad, Confidencialidad e Integridad de la información), se tiene que 18 son de Integridad (los que se asocian a riesgos de fugas de información, manipulación de información, etc.), 8 de Confidencialidad (ofuscación u ocultación de información confidencial como el R.U.T, número de tarjeta de crédito, entre otros) y 4 de Disponibilidad de la información, como se puede ver en el gráfico a continuación.

Figura 34 – Distribución tipos de riesgos (Pendientes) de proyectos 2018



Fuente: Elaboración Propia

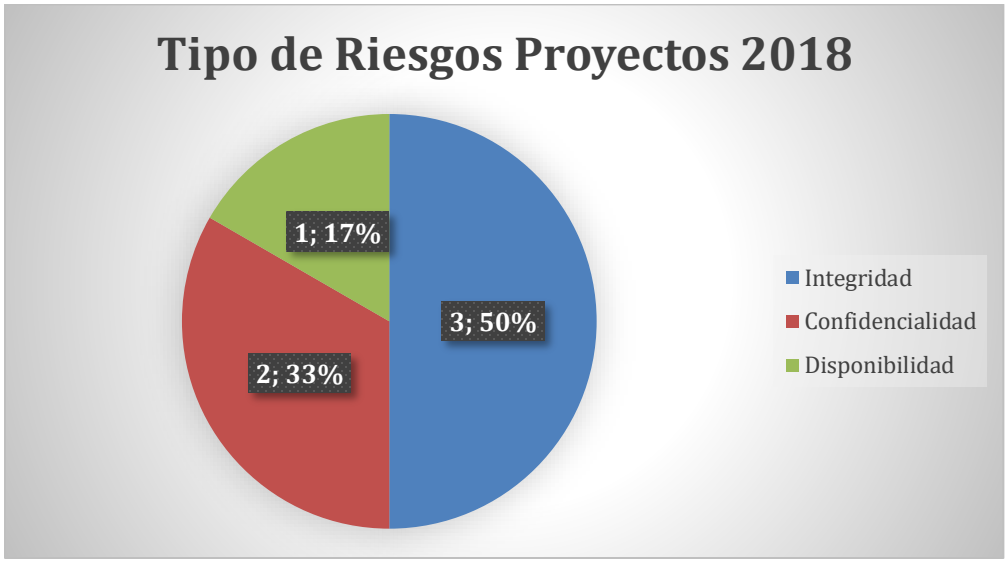
Para realizar una comparativa del periodo de prueba (Enero – Marzo 2019), en comparación con el mismo periodo durante el año 2018, se mostrará la información respecto al trimestre Enero – Marzo del año 2018. Durante este periodo, se presentaron 20 proyectos, de los cuales se encontraron 6 vulnerabilidades distribuidas de la siguiente forma:

Tabla 20 – Cantidad de riesgos (Enero – Marzo) 2018 según criticidad

Criticidad Riesgo	Cantidad
Crítico	0
Elevado	1
Moderado	5
Bajo	0

Fuente: Elaboración Propia

Figura 35 – Cantidad de riesgos (Enero – Marzo) 2018 por tipo



Fuente: Elaboración Propia

Como se puede visualizar en la tabla y gráfico anterior, se tiene los riesgos asociados al primer trimestre del año 2018, del cual, de un total de 20 proyectos durante ese periodo, un 83% de los riesgos son de carácter elevado, mientras que un 17% pertenecen a vulnerabilidades de riesgo medio. Así también, de estos riesgos un 50% son de integridad de la información, un 33% de confidencialidad, y un 17% de disponibilidad de la información.

6.2 Resultados Actuales

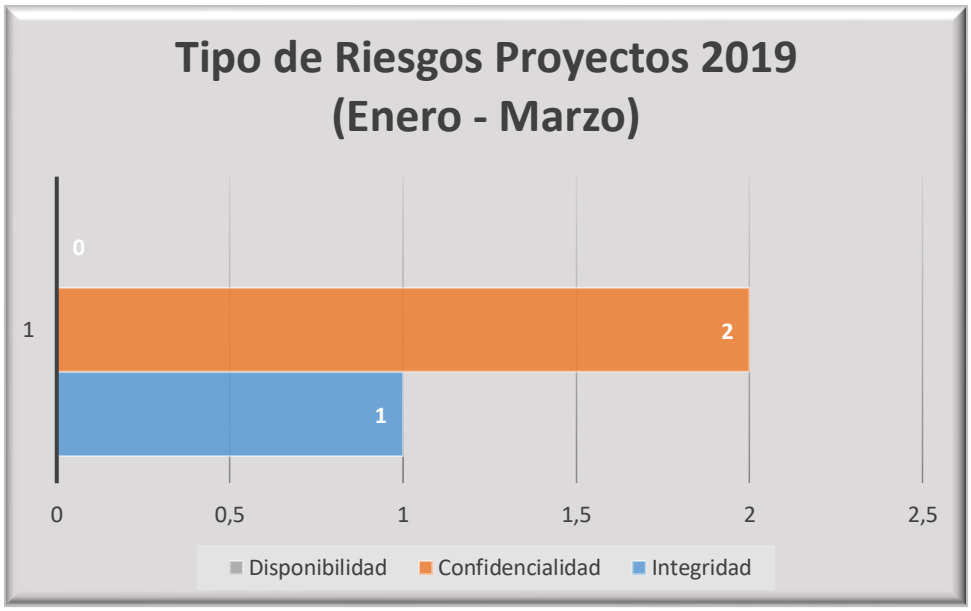
Durante el periodo de prueba, se presentaron a comisiones 26 proyectos (presentados en distintas etapas de estos mismos), de los cuales se identificaron 3 riesgos. A continuación, en la siguiente tabla y gráficos se podrá visualizar claramente los tipos de riesgos, su nivel de criticidad, entre otros.

Tabla 21 – Cantidad de riesgos (Enero – Marzo) 2019 según criticidad

Criticidad Riesgo	Cantidad
Crítico	0
Elevado	2
Moderado	1
Bajo	0

Fuente: Elaboración Propia

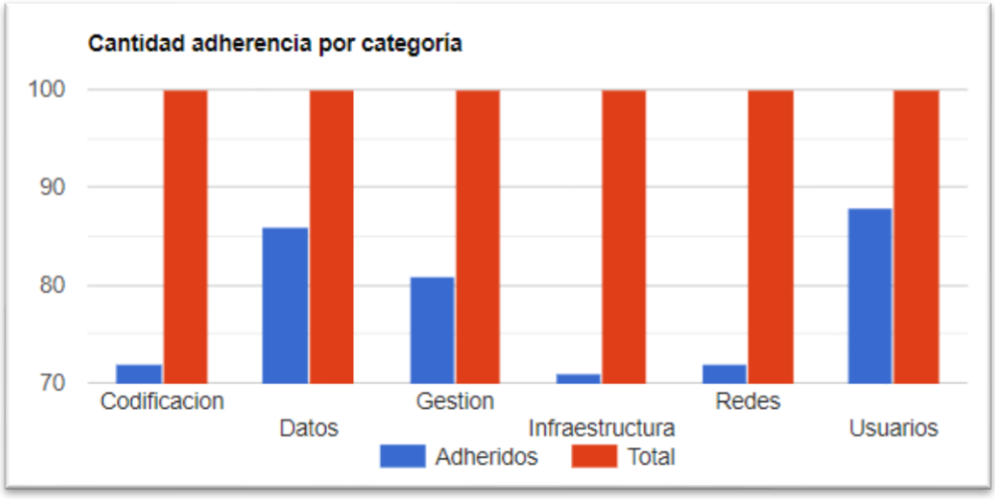
Figura 36 – Cantidad de riesgos (Enero – Marzo) 2019 por tipo



Fuente: Elaboración Propia

Por otra parte, en la plataforma, los resultados obtenidos se presentarán a continuación en los siguientes gráficos:

Figura 37 - Gráfico de Adherencia de controles por categoría



Fuente: Elaboración Propia

Según el gráfico anterior se puede visualizar el porcentaje de adherencia de controles según su categoría, respecto al total de controles de cada categoría, los cuales se distribuyen de la siguiente forma:

Tabla 22 – Distribución de adherencia a controles por categoría

Categoría	%Adherencia	%Total
Codificación	72%	100%
Datos	86%	100%
Gestión	81%	100%
Infraestructura	71%	100%
Redes	72%	100%
Usuarios	88%	100%

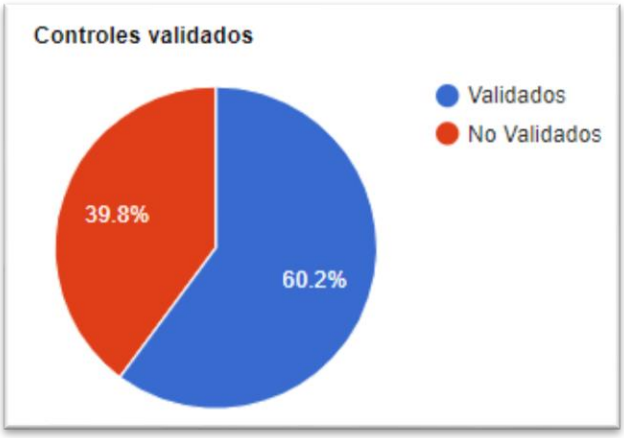
Fuente: Elaboración Propia

De los resultados anteriores, se puede visualizar que en todas las categorías existe una carencia en la adherencia de estos controles, principalmente a los controles asociados a redes, infraestructura y codificación. Esto se debe principalmente a la carencia de recursos asignados por la organización principalmente en términos de seguridad de la información, como también la carencia de personas especializadas en el área en los grupos de desarrollo de software, ya que en el ámbito en el que se probó el

sistema, los grupos de desarrollo son los encargados de coordinar y velar por reunirse con personal de seguridad de la información para ser ayudados en temas relacionados a seguridad, lo que genera una mayor incertidumbre al momento de ser presentados en comisión teniendo una mayor probabilidad de rechazo o quedar “pendiente de aprobación” y retrasando así el proyecto.

Por otra parte, en resumen, la adherencia de controles validada por el Jefe de seguridad se distribuyen de la siguiente forma:

Figura 38 – Gráfico de Validación de controles



Fuente: Elaboración Propia

En el gráfico anterior, se puede visualizar la distribución de la validación de los controles de seguridad de la información, en esto se tiene casi un 40% de controles no validados, esto principalmente al tiempo requerido para realizar estas validaciones, ya que estos deben ser validados por el encargado del proyecto mediante alguna evidencia que respalde la adherencia de este, por lo que algunos proyectos no tienen todos sus controles validados.

6.3 Análisis de Resultados

Respecto a los objetivos específicos planteados para el presente proyecto (Véase tabla 1.2), se obtuvieron los siguientes resultados:

Tabla 23 - Cumplimiento métricas por objetivos específicos

O. Específico	Métrica	VAM	CEM	¿Cumple?
O.E01: Entregar lineamientos básicos que se deben contemplar para un desarrollo seguro de software.	Determina la cantidad de vulnerabilidades de carácter medio, alto o crítico presentes en un proyecto de software, el cual será basado una metodología de desarrollo seguro, mediante un Ethical hacking (EH) y/o un escáner de vulnerabilidades (VA).	3 vulnerabilidades en total	$Cv \leq 3$ en promedio (basada en críticas, altas, medias)	✓
O.E02: Proveer información sobre la importancia de la seguridad de la información en el desarrollo de aplicaciones mediante un plan de sensibilización sobre la seguridad de la información.	Cantidad de reuniones o charlas en un mes.	3 en total (1 por mes)	$Cr \geq 1$ por mes	✓
O.E03: Proveer un checklist de las tareas que debe contemplar un software seguro.	Entregar un conjunto de buenas prácticas que al menos deben considerarse en un ciclo de desarrollo de software seguro	1	Checklist de los controles mínimos que debe cumplir un software seguro.	✓

Fuente: Elaboración Propia

De la tabla anterior, se puede visualizar el cumplimiento de los objetivos específicos planteados, donde se puede visualizar que el objetivo 1 se cumple, ya que existe una reducción respecto el primer trimestre del 2018 y del 2019, reduciéndose de 6 a 3

vulnerabilidades. Respecto al objetivo 2, se realizaron 3 eventos relacionados con sensibilización sobre seguridad de la información, de los cuales una fue una charla sobre fraude por phishing, posteriormente se realizó un ataque simulado de phishing, para realizar un análisis posterior respecto a sus resultados y finalmente se realizó una presentación final que ratifique la importancia de la seguridad de la información y los resultados obtenidos de la simulación realizada durante el mes de Febrero, cumpliendo finalmente con el objetivo 2 propuesto. Finalmente, para el objetivo 3 se realizó la entrega de un checklist de seguridad de la información, con los controles priorizados según su relevancia durante las diversas etapas de desarrollo de un software, además de la entrega de la plataforma web en la que se puede hacer seguimiento a la adherencia de controles en los diversos proyectos (donde igualmente se puede visualizar el checklist), por lo que se cumple con este y todos los objetivos específicos presentados durante el presente informe.

Respecto a los resultados, si bien los datos demuestran una reducción de la cantidad de vulnerabilidades, ya que, en promedio en el periodo de prueba del 2019 de 26 proyectos, se encontraron 3 vulnerabilidades, esto significa que aproximadamente en un 12% de los proyectos se identificaron vulnerabilidades durante las comisiones de evaluación de proyectos, equivalente a 3 proyectos con vulnerabilidades, mientras que en el 2018 de 148 proyectos, de los cuales un 20.3% del total de proyectos se les identificaron vulnerabilidades, equivalente a 30 proyectos. Estos datos demuestran que hubo una mejora, sin embargo, pueden no ser muy verídicos, ya que se está comparando un período de prueba de 3 meses, contra un año completo, lo que puede afectar al análisis de resultado. Por esta razón, se realizó la comparación del mismo periodo respecto al 2018 v/s el 2019, donde se obtienen los siguientes resultados:

- Durante el año 2018 de un total de 20 proyectos en ese periodo, se encontraron 6 vulnerabilidades, con lo que se obtiene que en el 30% de los proyectos se encontraron vulnerabilidades, equivalente a 6 proyectos.

- Durante este mismo trimestre respecto al año 2019, de un total de 26 proyectos, se encontraron 3 vulnerabilidades, correspondiente al 12% de los proyectos, lo cual equivale a 3 proyectos.

Dicho lo anterior, se tiene una reducción de las vulnerabilidades durante el periodo de prueba, por lo que dado estos resultados y el cumplimiento de los objetivos específicos, es que se determina refutar la hipótesis nula, validando así que una metodología enmarcada en el desarrollo seguro de software si es capaz de reducir la cantidad de vulnerabilidades que se pueden materializar en un futuro.

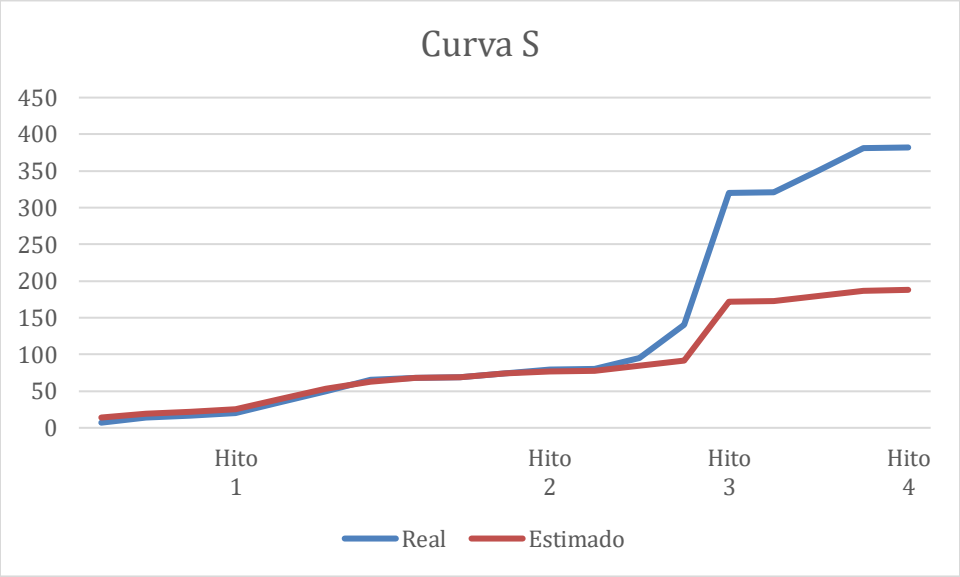
6.4 S2D2 v/s Propuesta Actual

Como ya fue mencionado durante el estado del arte, a comparación con la otra propuesta S2D2, en el proyecto propuesto, claramente se busca concientizar al grupo de trabajo sobre la seguridad de la información, de hecho, se entrega una plataforma que permita no solo evaluar al equipo de trabajo, sino que también entregarle un video previo a las evaluaciones, que complementen las concientizaciones realizadas en la organización. Por otra parte, igualmente se está entregando una interfaz de seguimiento de la metodología, de hecho, a modo de comparación esta es mucho más amigable y acotada que la propuesta de S2D2 (Ver anexo A5 para visualizar imágenes de la propuesta S2D2 y A6 para la propuesta actual). En cuanto, al tercer punto mencionado durante el estado del arte, S2D2 se enfoca en las metodologías de trabajo tradicionales, mientras que la propuesta actual, como ya se mencionó, se ocupa la estructura de Scrum, añadiendo características importantes de PMBOK, como también metodologías seguras como Secure Scrum y DevSecOps. Finalmente, ambas propuestas entregan un checklist basados en diversas normas asociadas a controles de seguridad de la información. Sin embargo, la propuesta presentada en este proyecto, a diferencia de S2D2, solo se consideraron los controles más críticos en cada etapa del proyecto, además reunir y resumir controles similares entre las diversas normas, con tal de que sea más cómodo

para el usuario de leer e interpretar que tener muchos controles. Cabe mencionar, que se descartan llevar en el checklist todos los controles, ya que será tedioso para el usuario que deba aplicar esta metodología, como también, si bien todos los controles de seguridad de la información tienen igual importancia, estos se clasifican por criticidad, siendo así los críticos los que se deben dar mayor prioridad de implementar, primeramente.

6.5 Curva de Desempeño (Curva S)

Figura 39 – Curva de Desempeño



Fuente: Elaboración Propia

En la figura 39, se puede visualizar la curva de desempeño del proyecto, en donde se puede apreciar que durante Hito 1 y 2 se tuvo un rendimiento acorde al estimado, en ocasiones por sobre lo estimado. Sin embargo, desde el Hito 3 hasta el fin del proyecto, se dispara totalmente la brecha entre lo real y lo estimado, lo cual se debe a diversos factores, tales como complicaciones en el desarrollo de la plataforma web, principalmente por falta de conocimiento en la realización de estas, así también otros factores externos dificultaron la posibilidad de probar en un entorno real la propuesta desarrollada en el

periodo estimado y durante un periodo que se considere adecuado para obtener buenos resultados.

6.6 Conclusiones

A lo largo del presente informe de tesis, se pudo evidenciar las principales falencias que genera el desarrollo de software sin considerar la seguridad de la información como un factor esencial en este, así también, diversos ejemplos que evidenciaban los costos que significan para las organizaciones un ataque en su sistema por alguna vulnerabilidad. Por esta razón, es de total importancia que la seguridad de la información sea un factor esencial, siempre dependiendo del negocio, pero si debe ser aplicado en cualquier tipo de proyecto informático, ya sea, para el ámbito financiero, de entretenimiento (videojuegos) o incluso sistemas mucho más críticos como los sistemas informáticos de los aviones, el que puede incluso poner en riesgos vidas de personas. Así también, se pudo ver que a comparación con las propuestas similares, este proyecto si considera una plataforma que sea fácil de usar para el usuario, además de entregar un checklist con los controles con mayor prioridad al momento de desarrollar cualquier software y/o aplicativo, para que el equipo de trabajo sea capaz de retener estos controles, además que los tomen en consideración y no sea una molestia ni una gran pérdida de tiempo para el usuario que deba aplicar controles mínimos de seguridad de la información en un proyecto.

En base a los resultados obtenidos, se puede evidenciar que se cumple con los objetivos específicos del presente proyecto, sin embargo, no se aplicó todo como se esperaba, como en el caso de las presentaciones de concientizaciones, en las que se abarcaron un grupo reducido de personas (sin considerar los que no asistieron respecto al total de invitados), esto dado a la falta de tiempo para realizar un proceso que puede llevar mucho tiempo en cumplir su objetivo como tal, debido a la gran cantidad de colaboradores en la entidad financiera en la que se probó, así como los recursos que

dispone la empresa para llevar esto a cabo. Así también, la poca duración del periodo de prueba de la metodología fue un factor en contra, ya que como aplica a diversos proyectos, es difícil obtener conclusiones “apresuradas” sin realizar el seguimiento desde el inicio hasta el fin de diversos proyectos, sin embargo, se normalizaron los datos obtenidos, para realizar una comparación entre ambos periodos. También, factores como el período en el cual se probó pudieron influir en los resultados, ya que se evidenció que durante el periodo de Verano 2019 (Enero – Marzo) existió una baja en la cantidad de proyectos que se presentaron a comisiones a diferencia de otros periodos del año.

Dado lo anterior, y considerando los resultados obtenidos del primer trimestre del 2018 y 2019, se decide concluir con que se cumple el objetivo principal del presente trabajo, refutando la hipótesis nula, y concluyendo así que una metodología de trabajo enmarcada en la seguridad de la información es capaz de reducir los riesgos que se pueden materializar en un futuro, posterior al desarrollo de un software u aplicativo, esto debido principalmente a que se cumplió el objetivo principal de reducir las vulnerabilidades de los proyectos,

6.7 Trabajos Futuros

Como trabajos futuros, es deseable realizar pruebas de la metodología nuevamente durante un tiempo más amplio el que permita obtener resultados significativos de este (que implique todo el proceso de inicio y fin de diversos proyectos de software) así como también implementar el plan de concientización idealmente a toda la organización, lo que permitiría reducir en mayor porcentaje los riesgos. Respecto a futuras implementaciones, se desea la capacidad de hacer seguimiento a las actividades que realizan los trabajadores en el desarrollo del proyecto, en el que cada usuario ingrese la actividad que está realizando, lo que realizó en el día, etc., para así medir el desempeño de estos, y conocer si están adhiriéndose a los controles de seguridad de la información como se espera y no solo porque debe de cumplir con estos.

6.8 Glosario

CEM: Criterio de éxito de la métrica.

VAM: Valor actual de la métrica.

Hardening: Es un proceso que se encarga de asegurar un sistema, mediante la reducción de vulnerabilidades en este, ya sea, eliminando software, servicios, usuarios, así como el manejo de puertos, gestión de permisos de usuarios, entre otros (Grupo Smartekh, 2012).

QA & Testing: En español conocido como Pruebas y aseguramiento de calidad, consiste a las fases de probar un sistema durante el desarrollo, con tal de detectar fallos, para ser informados y resueltos, mientras que QA (Quality Assurance) se conoce como un conjunto de actividades que tienen como fin asegurar la calidad de un software, durante las diversas fases de su desarrollo (Márquez, 2017).

6.9 Referencias

Álvarez, R. (07 de 08 de 2017). Xataka. Obtenido de Los datos de 143 millones de personas filtrados ante el hackeo a Equifax, una de las mayores agencias crediticias: https://www.xataka.com/seguridad/hackean-equifax-una-de-las-mayores-agencias-de-informes-crediticios-afectando-a-143-millones-de-usuarios

Arroyo, R. (21 de 02 de 2011). ITespresso. Obtenido de Software inseguro, clave en la creación de vulnerabilidades: https://www.itespresso.es/software-inseguro-clave-en-la-creacion-de-vulnerabilidades-49592.html

Bairwa, S., Mewara, B., & Gajrani, J. (2014). VULNERABILITY SCANNERS: A PROACTIVE APPROACH TO ASSESS WEB APPLICATION SECURITY. International Journal on Computational Sciences & Applications (IJCSA), 1-12.

bccResearch. (s.f.). bccResearch. Obtenido de About Us - bccResearch: https://www.bccresearch.com/aboutus

Consumer Reports. (20 de 02 de 2018). La Opinion. Obtenido de https://laopinion.com/2018/02/20/estas-dos-televisiones-inteligentes-son-vulnerables-a-la-pirateria/

Creative Intellect Consulting (CIC). (s.f.). Creative Intellect Consulting (CIC). Obtenido de https://www.creativeintellectuk.com/about-cic

Dana, C. (22 de 02 de 2017). Blog Impulse. Obtenido de https://blog.impulse.pe/6-pasos-para-crear-un-plan-de-marketing-de-contenidos

Deemer, P., Benefield, G., Larman, C., & Vodde, B. (2010). Goodagile. Obtenido de The Scrum Primer: http://goodagile.com/scrumprimer/scrumprimer.pdf

Dreamlab Technologies. (s.f.). Dreamlab Technologies. Obtenido de Acerca de Nosotros: https://dreamlab.net/es/dreamlab/

EIU Inclusive Internet Index. (2018). EIU Inclusive Internet Index. Obtenido de https://theinclusiveinternet.eiu.com/explore/countries/performance

GlobalSTD. (23 de 10 de 2018). GlobalSTD Certification. Obtenido de ISO Survey 2017: https://www.globalstd.com/networks/blog/iso-survey-2017

Grupo Smartekh. (03 de 05 de 2012). Blog Smartekh. Obtenido de ¿QUÉ ES HARDENING?: http://blog.smartekh.com/que-es-hardening

HCL Software. (2019). HCL Technologies. Obtenido de HCL APPScan: https://www.hcltechsw.com/wps/portal/products/products-home/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zi_QO8nQ0MnQ0CLMzCzA0CHf08Q8IsnQwNzM31w9EUOAa5ABV4ulsG-7obGZiY6kcRo98AB3A0IE4_HgVR-I0P149CswLVB94mBBSAvEjIkoLc0NAIg0xPAJYe1HQ!/?1dmy&urile=wcm%3apath%3a/wps

HCL Software. (2019). HCL Technologies. Obtenido de HCL AppScan Source: https://www.hcltechsw.com/wps/portal/products/appscan/home/!ut/p/z1/lZJNc4IwEIb_ij14ZDZCIHJEnLFKrVYEJZdO-IjQSkBMtf33DTO92I5Yc8vss7PvPLtAYQtUsFOxY7KoBNurf0St18XSc9HARcvF2HLRizN3Pf8pNPAMw-YSGDqrsQKmE9ufT3SETaAXZSskqvw8XYf2aIAI-elHV56D_tffAdDu_CFQoHVSpBARRgz

Hernández Sampieri, R., Fernández Collado, C., Baptista Lucio, P., Méndez Valencia, S., & Mendoza Torres, C. (2014). Metodología de la investigación. 5th ed. México. McGraw-Hill Education.

Hevia, A., & Riveros, E. (2018). OWASP LATAM 2018. Obtenido de OWASP Latin America Tour: https://adderou.cl/posts/presentacion-owasp-tus-compras-gratis/

HTBridge. (s.f.). ImmuniWeb. Obtenido de ImmuniWeb® AI Platform: https://www.htbridge.com/immuniweb/

HuffPost. (20 de 07 de 2015). HuffPost. Obtenido de Un ciberataque a la web de contactos Ashley Madison amenaza datos de miles de clientes: https://www.huffingtonpost.es/2015/07/20/ataque-ashley-madison_n_7832714.html

InfoeducativaDigital. (26 de 09 de 2017). InfoeducativaDigital. Obtenido de http://infoeducativadigital.blogspot.com/2017/09/caracteristicas-del-enfoque-cuantitativo.html

Iñaki, M. (05 de 2015). Openmet Group. Obtenido de Cómo superar la desmotivación laboral a través de la comunicación: https://www.openmet.com/como-superar-la-desmotivacion-laboral-a-traves-de-la-comunicacion.htm/

ISO27000. (2017). ISO27000. Obtenido de http://iso27000.es/iso27002

ISOTools. (06 de 2014). SGSI - Blog especializado en Sistemas de Gestión de Seguridad de la Información. Obtenido de ISO 27001 – ¿Cómo confeccionar un plan de concienciación sobre la Seguridad de la Información?: https://www.pmg-ssi.com/2014/06/iso-27001-como-confeccionar-un-plan-de-concienciacion-sobre-la-seguridad-de-la-informacion/

ISOTools. (2017). ISOTools. Obtenido de La norma ISO 27001 - Aspectos clave de su diseño e implantación: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

ITSec. (s.f.). ITSec. Obtenido de Nuestra Empresa: https://www.itsec.cl/nosotros

Kruchten, P. (1995). Planos Arquitectónicos: El Modelo de "4+1" Vistas de la Arquitectura de Software. IEEE Software 12. Obtenido de http://cic.puj.edu.co/wiki/lib/exe/fetch.php?media=materias:modelo4_1.pdf

Lapena, R. (13 de 03 de 2017). Tripwire. Obtenido de More than 90% of IT Pros Expect More Attacks, Risk, and Vulnerability with IIoT in 2017: https://www.tripwire.com/state-of-security/featured/90-pros-expect-attacks-risk-vulnerability-iiot-2017/

Lopez Provencio, F. (2015). Metodologías para el desarrollo seguro de software. Barcelona: Facultad de Informática de Barcelona.

Lopez, E. (2016). Crowdlending.es. Obtenido de https://www.crowdlending.es/blog/que-es-fintech

M. Rayo, Á. (21 de 07 de 2016). Bit Computer Training. Obtenido de Principales retos de seguridad en proyectos Big Data:

https://www.bit.es/knowledge-center/principales-retos-seguridad-big-data/

Márquez, R. (23 de 03 de 2017). Paradigma Digital. Obtenido de Blog Tecnología para Desarrollo: https://www.paradigmadigital.com/dev/tester-vs-quality-assurance/

OWASP. (2017). OWASP. Obtenido de OWASP Top 10 - 2017 - The Ten Most Critical Web Application Security Risks: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Paul Hammant. (1 de 11 de 2012). Paul Hammant's blog. Obtenido de https://paulhammant.com/2012/11/01/testability-and-cost-of-change/

PCI Security Standards Council. (04 de 2016). PCI Security Standards. Obtenido de Industria de Tarjetas de Pago (PCI) - Norma de seguridad de datos: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2es-LA.pdf

Peña, J. C. (27 de 06 de 2017). Techbit - El Universal. Obtenido de Los 7 mayores ciberataques de la historia: https://www.eluniversal.com.mx/articulo/techbit/2017/06/27/los-7-mayores-ciberataques-de-la-historia

Pohl, C., & Holf, H.-J. (2015). Secure Scrum: Development of Secure Software. Securware 2015, 1-6.

Raynaud, F. (2017). DevSecCon. Obtenido de DevSecOps Whitepaper - The business benefits and best practices of DevSecOps implementation: https://www.devseccon.com/wp-content/uploads/2017/07/DevSecOps-whitepaper.pdf

Retos en Supply Chain. (17 de 11 de 2017). EAE Business School - Retos en Supply Chain. Obtenido de Qué es la guía PMBOK y cómo influye en la administración de proyectos: https://retos-operaciones-logistica.eae.es/que-es-la-guia-pmbok-y-como-influye-en-la-administracion-de-proyectos/

Rios, F. (30 de 09 de 2016). Revista IT. Obtenido de 10 CIBERATAQUES MAS FAMOSOS DE LA HISTORIA: http://www.revistait.cl/bi/tendencia-e-innovacion/item/964-10-ciberataques-mas-famosos-de-la-historia

Rouse, M. (2012). TechTarget. Obtenido de Los 12 requisitos PCI DSS: https://searchdatacenter.techtarget.com/es/definicion/Los-12-requisitos-PCI-DSS

Ruiz, Y., Zulueta, Y., & Gainza, D. (05 de 2007). Gestión de Proyectos Informáticos. Obtenido de https://slideplayer.es/slide/71845/

Sahare, B., Naik, A., & Khandey, S. (2014). Study of Ethical Hacking. International Journal of Computer Science Trends and Technology (IJCST), 1-5.

Sassone, S. (16 de 08 de 2016). WeliveSecurity by Eset. Obtenido de Por qué la seguridad es transversal al desarrollo de videojuegos: https://www.welivesecurity.com/la-es/2016/08/16/seguridad-desarrollo-de-videojuegos/

Scrum.org. (2015). Scrum.org. Obtenido de https://metodologiascrum.readthedocs.io/en/latest/Scrum.html

Subsecretaría de Telecomunicaciones. (Marzo de 2019). Subtel - Sector Telecomunicaciones Cierre 2018. Obtenido de https://www.subtel.gob.cl/wp-content/uploads/2019/04/PPT_Series_DICIEMBRE_2018_V2.pdf

Tenable. (2018). Tenable. Obtenido de Nessus: https://www.tenable.com/products/nessus/nessus-professional

Toro, R. (28 de 09 de 2017). SGSI - Blog especializado en Sistemas de Gestión de Seguridad de la Información. Obtenido de ¿Cuál es la situación de la norma ISO 27001 en Sudamérica?: https://www.pmg-ssi.com/2017/09/situacion-norma-iso-27001-sudamerica/

Velykholova, Y. (11 de 08 de 2017). N-iX. Obtenido de 5 Tech Innovations Behind Modern IoT Security Solutions: https://www.n-ix.com/5-tech-innovations-behind-modern-iot-security-solutions/

Winkler, V. (22 de 08 de 2016). Microsoft. Obtenido de Cloud Computing: Problemas de seguridad de nube: https://docs.microsoft.com/es-es/previous-versions/technet-magazine/hh536219(v=msdn.10)

6.10 Anexo

A1. Checklist de conjunto de buenas prácticas y controles mínimos para un desarrollo seguro de software.

Tabla 24 – Checklist controles y buenas prácticas para un desarrollo seguro de software

Categoría	Controles	Descripción	¿Se adhiere?	¿Por qué?
Gestión	Gestión de personal o contratación	Se debe contratar personal calificado para el rol que se necesita en el desarrollo del proyecto, para así obtener los resultados esperados de este. Nota: Cabe destacar que no necesariamente el personal a contratar debe ser experto en el área que se desempeñará, ya que se puede capacitar al personal que se está contratando, pero si debe cumplir con los valores propuestos de la organización.		
Gestión	Clasificación de la información y acuerdos de confidencialidad	La información manipulada debe ser clasificada según sus requisitos legales, valor, criticidad y sensibilidad frente a la divulgación o modificación sin previa autorización. Así también, se deben realizar y documentar acuerdos de confidencialidad, de acuerdo con la información que se está manejando.		
Gestión	Concientización sobre la seguridad de la información	Es importante concientizar periódicamente a los colaboradores sobre la seguridad de la información, con temas como el impacto que genera una mala manipulación de datos sensibles como también la exposición de estos. Además, se debe actualizar a los trabajadores sobre las ultimas vulnerabilidades, como en el caso del desarrollo web con OWASP Top 10. Nota: Es importante considerar que la concientización a los colaboradores debe ser según las habilidades de estos, por tanto, es recomendable dividir los temas del plan de concientización según las habilidades de cada grupo de trabajadores, como por ejemplo, en el caso de las vulnerabilidades en el desarrollo web que ofrece OWASP, estos temas son principalmente de interés para los programadores. Cabe destacar, que con este plan de concientización se puede realizar un análisis sobre los temas que los trabajadores no se están adhiriendo correctamente, por lo que se puede priorizar en reforzar estos temas.		

Fuente: Elaboración Propia

Tabla 24 – Checklist controles y buenas prácticas para un desarrollo seguro de software (Continuación)

Categoría	Controles	Descripción	¿Se adhiere?	¿Por qué?
Gestión	Documentación y justificación del negocio para el uso de los servicios, protocolos y puertos permitidos	Es estrictamente necesario que en un sistema y/o software a desarrollar, todos los protocolos, servicios y puertos utilizados, tanto inseguros como seguros, sean justificados para el negocio, y verificados que se les haya implementado funciones de seguridad para cada uno. Además, estos deben estar documentados. Por otra parte, se deben utilizar solo los necesarios para las funciones del sistema.		
Gestión	Inventario de dispositivos y software	Es importante llevar un inventario de los equipos que se utiliza en la organización, con tal de identificar los equipos no autorizados. Además, se debe llevar un inventario de los softwares que son necesarios para desarrollar el trabajo de los colaboradores, para así bloquear cualquier otro programa.		
Gestión	Seguridad en el área de trabajo	Se deben establecer reglas en el área de trabajo de los colaboradores, tales como la instalación de software y accesos a sitios no seguros, con tal de no penetrar la red o algún equipo de trabajo, mediante un proceso de Hardening. Además, se debe controlar el acceso de los dispositivos extraíbles, tales como memoria USB o discos duros externos, y en el caso de ser necesario se deben encriptar todos los datos de estos. Entre otras buenas prácticas asociadas a la seguridad en el área de trabajo se tienen: - Eliminar todo driver y software innecesario, como también limitar el acceso a determinadas herramientas de scripting como Powershell o Python para evitar posibles vulnerabilidades de estas partes. - Se recomienda utilizar un software anti-malware de gestión centralizado (como por ejemplo Kaspersky Security Center), para monitorear y defender todos los equipos y servidores en la organización, realizando análisis de estos equipos y actualizarlos, para detectar y controlas amenazas más recientes. - Se recomienda mantener las últimas actualizaciones de seguridad de los diversos software y S.O utilizado, además de mantener actualizada la base de datos del software de anti-virus utilizado para que sea capaz de detectar las nuevas amenazas reportadas día a día.		
Gestión	Controles contra código malicioso	Se deben implantar controles de detección, recuperación y prevención, junto con concientización a los usuarios, para protegerse de los códigos maliciosos, tales como virus, troyanos, gusanos, bots o malwares. Para esto, se puede aplicar diversos softwares para la detección y mitigación de estos, como por ejemplo Kaspersky Anti-Virus y Kaspersky Internet Security.		

Fuente: Elaboración Propia

Tabla 24 – Checklist controles y buenas prácticas para un desarrollo seguro de software (Continuación)

Categoría	Controles	Descripción	¿Se adhiere?	¿Por qué?
Gestión	Diagrama de flujo de datos	Es importante que exista un diagrama con el flujo de los datos que se utilizaran en el sistema a implementar con tal de conocer con qué otros sistemas se comunicarán y finalmente donde se almacenará este.		
Gestión	Monitoreo de configuraciones del sistema	Implementar un sistema de monitoreo compatible con el protocolo Security Content Automation Protocol (SCAP) que verifique constantemente las configuraciones, y alerte en el caso de una modificación no autorizada en estas.		
Gestión	Seguridad en la implantación de un sistema	En todo sistema previo a implantar, siempre es necesario cambiar las contraseñas por defecto entregada por los proveedores de servicios, software o equipos, por tanto, es estrictamente necesario probar que no se puede acceder a estos por ninguna credencial por defecto. Además, previo a la implantación de un sistema, es necesario implementar un plan de respuesta ante incidentes para responder ante un fallo en este.		
Gestión	Seguridad de los proveedores	Los requisitos de seguridad de la información deben ser definidos y acordado con los proveedores que puedan acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la organización. Además, estos deben ser supervisados periódicamente.		
Gestión	Gestión de cambios	Se debe gestionar todo cambio a realizar durante un desarrollo de software, o en el caso algún requisito o funcionalidad post-desarrollo, con tal de analizar y verificar que no afecte en el resguardo de la información. Esto se puede llevar a cabo con un control de cambio para el proyecto o el sistema que se está desarrollando.		
Infraestructura	Seguridad en servidores	Es recomendable implementar una sola función por servidor, así también, en el caso de virtualización solo una por dispositivo virtual, con la finalidad enfocarse en un solo nivel de seguridad para cada función. Nota: En el caso de tener todas las funciones en un mismo servidor reducirá la efectividad de este, llegando a ser más vulnerable.		
Infraestructura	Seguridad física de oficinas, salas e instalaciones	Se debe aplicar la seguridad en las oficinas, salas u otras instalaciones, con tal de protegerse contra la falla de equipamientos por suministro de energía u otros incidentes, por lo que es importante proteger los cableados y mantenimiento adecuado de los equipos, además de poseer componentes u equipos redundantes en caso de fallo para que estos estén la mayor parte del tiempo disponible.		
Redes	Seguridad en los servicios de correos electrónicos	En el caso de utilizar servicios de correo electrónicos para la comunicación con el grupo de trabajo, proveedores u otras partes, se recomienda utilizar técnicas de sandboxing para analizar y bloquear correos con archivos adjuntos de carácter malicioso.		

Fuente: Elaboración Propia

Tabla 24 – Checklist controles y buenas prácticas para un desarrollo seguro de software (Continuación)

Categoría	Controles	Descripción	¿Se adhiere?	¿Por qué?
Redes	Controles de red	Las redes se deben gestionar y controlar para resguardar la información en los sistemas y aplicaciones, para esto, se recomienda las siguientes herramientas y buenas prácticas para el control de acceso a la red en la organización: - Utilizar un firewall que permita filtrar las conexiones no seguras al sistema. - Utilizar servicios de filtro de DNS para ayudar a bloquear algunos dominios maliciosos ya conocidos, como también, denegar conexiones por puertos no autorizados. - Asegurar que todo tráfico de red hacia o desde Internet pase por un proxy configurado para filtrar conexiones no autorizadas. - En el caso de redes inalámbricas, se recomienda utilizar un sistema inalámbrico de detección de intrusos (WIDS) para alertar sobre accesos no autorizados a la red. - Utilizar el estándar de cifrado avanzado (AES 256) para cifrar los datos en tránsitos en una red inalámbrica. - Se recomienda la utilización de protocolos de autenticación como EAP/TLS para redes inalámbricas, la que requiere autenticación de múltiples factores. - Se recomienda limitar el acceso a la red a cualquier equipo que no cumpla un propósito definido para la organización.		
Redes	Seguridad de las comunicaciones en servicios accesibles por redes públicas	En el caso de servicios accesibles por redes públicas u externas, la información utilizada en estos servicios se debería proteger de divulgación o reproducción para usos fraudulentos. Para esto se puede aplicar una zona desmilitarizada (DMZ), con tal de que se puedan proveer servicios desde la red interna hacia el exterior, pero sin acceso a la red interior.		
Usuarios	Control de login y modificación de permisos	Como buena práctica, se recomienda que, para todo ingreso de usuarios al sistema, se habilite un registro de log con al menos la fecha, hora, origen, usuario, tipo de evento, indicación de éxito o fallo de la tarea realizada, y componentes o recursos afectados en el sistema al momento de ingresar un usuario y/o realizar diversas tareas o transacciones dentro del sistema. También, se recomienda tener un registro de cualquier modificación realizada en los permisos de los usuarios. Notas: Esta práctica puede servir para realizar un análisis en el caso del ingreso de una persona malintencionada en el sistema.		

Fuente: Elaboración Propia

Tabla 24 – Checklist controles y buenas prácticas para un desarrollo seguro de software (Continuación)

Categoría	Controles	Descripción	¿Se adhiere?	¿Por qué?
Usuarios	Registro, manejo y eliminación de usuarios	Es necesario crear procedimientos para el registro y eliminación de usuarios, para controlar el acceso, como también para la asignación y modificación de permisos de estos, con tal de controlar el acceso al sistema y a los servicios, y así evitar la manipulación de datos sensibles. Para la aplicación de estos procesos, se recomienda utilizar cuentas de administradores, para evitar una mala manipulación de estos procedimientos. Nota: Como buenas prácticas se recomiendan las siguientes: - Encriptar todas las credenciales de autenticación de usuarios al momento de ser almacenadas. - Ocupar autenticación de múltiples factores para las cuentas de administrador (por ejemplo, el autenticador de 2 factores (A2F), que es el comúnmente utilizado en la actualidad). - Utilizar las cuentas de administradores solo para estas tareas, como también utilizarlas solo en equipos dedicados exclusivamente para el uso administrativo. - Cifrar todo tipo de acceso administrativo que no sea de consola (como el protocolo SSL/TLS para cifrar información en aplicaciones web), para evitar un posible filtro de credenciales de administrador, que permitan hurtar o eliminar información.		
Usuarios	Seguridad de los usuarios	Es importante resguardar la seguridad de los usuarios que ingresan al sistema, por tanto como buenas practica se proveen las siguientes: - Solicitar al usuario ingresar nuevamente la contraseña para reactivar la sesión en caso de estar inactivo más de 15 minutos. - Dejar ilegible las credenciales de autenticación mediante un método de criptografía sólido. - Verificar la identidad del usuario antes de modificar alguna credencial de autenticación. - La longitud de las contraseñas deben a lo menos tener 7 caracteres entre caracteres numéricos y alfabéticos. - No permitir el uso de una contraseña nueva que sea igual a las 4 últimas utilizadas. - Solicitar cambio de contraseña en el primer ingreso del usuario. - No utilizar ID y contraseñas genéricas ni compartidas. - En el caso de cuentas de usuario inactivas, se deben eliminar o inhabilitar, al menos al cabo de 90 días.		

Fuente: Elaboración Propia

Tabla 24 – Checklist controles y buenas prácticas para un desarrollo seguro de software (Continuación)

Categoría	Controles	Descripción	¿Se adhiere?	¿Por qué?
Datos	Controles criptográficos	Se debe asegurar el uso adecuado y eficaz de criptografía, para así proteger la confidencialidad, autenticidad e integridad de la información. Para esto, se recomienda utilizar algoritmos de encriptación estandarizados, tal como Secure Hash 2(SHA-2) o Secure Hash 3 (SHA-3).		
Datos	Seguridad en el acceso a las bases de datos	Es importante mantener la integridad de los datos almacenados en las bases de datos, utilizando aplicaciones para el monitoreo de los cambios que se generen en estos, tal como el File Integrity Manager (FIM) de Tripwire. Además, se debe considerar algunas buenas prácticas que permitan reducir el riesgo de afectar la integridad de la información, tal como: - Todo acceso o acciones de usuarios en las bases de datos se realizan únicamente mediante métodos programáticos, los cuales solo las aplicaciones pueden usar las ID de acceso para las bases de datos. - Solo los administradores de la base de datos pueden acceder directamente a las bases de datos o realizar consultas directamente en esta.		
Datos	Respaldo de la información	Se deben implementar métodos de respaldo automatizado de la información que la organización necesite almacenar. Además, debe asegurarse de cifrar o aplicar algún otro método de seguridad al momento de almacenar el respaldo, con tal de asegurar la integridad de estos.		
Datos	Control de retención de datos	Se deben definir una política de retención para los datos, junto con el tiempo durante el cual se mantendrán almacenados en caso de ser estrictamente necesario su almacenamiento, y en el caso contrario definir una política para su eliminación de manera segura.		
Codificación	Seguridad en la codificación	Es importante establecer practicas seguras de codificación, como la utilización de herramientas de análisis estático y dinámico de software, o la utilización de algoritmos de encriptación estandarizados. Además, es importante que previo al envío a producción o al momento de ponerse a disposición de los cliente, se revise el código para identificar posibles vulnerabilidades en la codificación mediante las siguientes recomendaciones: - La revisión de los códigos debe estar a cargo de personas que no hayan creado el código y tengan conocimientos en revisión de código y prácticas de codificación segura. - Las revisiones deben garantizar que el código se desarrolla de acuerdo a las directrices de codificación segura contempladas por la organización. - Las correcciones pertinentes se deben implementar antes del lanzamiento. - La gerencia debe revisar y aprobar los resultados de la revisión de códigos.		

Fuente: Elaboración Propia

Tabla 24 – Checklist controles y buenas prácticas para un desarrollo seguro de software (Continuación)

Categoría	Controles	Descripción	¿Se adhiere?	¿Por qué?
Codificación	Control de acceso al código fuente de los programas	Se debe restringir el acceso al código fuente del software o servicio que se está desarrollando, para así evitar la manipulación de personas maliciosas.		
Codificación	Pruebas de seguridad del sistema	Es necesario definir pruebas de aceptación sobre seguridad de la información con sus respectivos criterios. Además, se deben aplicar estas pruebas con el software o servicio que se está desarrollando para asegurar la correcta implementación de seguridad, de acuerdo con las políticas de la organización y legales. Nota: Es importante eliminar las cuentas de desarrollo, de prueba y de aplicaciones personalizadas, las ID de usuario y las contraseñas antes de que las aplicaciones se activen o se pongan a disposición de los clientes.		
Codificación	Herramientas de apoyo para detectar vulnerabilidades	Aplicar herramientas y técnicas de detección de vulnerabilidades, tales como pen-test (o Ethical hacking) y escáner de vulnerabilidades para detectar diversas brechas en el sistema y/o aplicación, y así trabajar en la mitigación de estos previo a la puesta en marcha, con tal de evitar la explotación de estas vulnerabilidades en un futuro. Nota: Entre las buenas prácticas asociadas al uso de estas herramientas y técnicas se tiene: - Utilizar un proceso de calificación de estas vulnerabilidades detectadas para priorizar la mitigación de las más críticas. - Eliminar o restablecer las cuentas de usuarios utilizadas por estas pruebas para detectar las vulnerabilidades, para evitar que se utilicen para otros fines. - Establecer un proceso que incluya un medio para que las entidades externas que realicen estas pruebas se comuniquen con el grupo de seguridad de la organización, para proveer el informe con las vulnerabilidades detectadas y tratarlas.		

Fuente: Elaboración Propia

A2. Plan de Concientización

Tabla 25 – Plan de concientización

	Actividades
Enero	Introducción sobre la importancia de la seguridad de la información y el impacto de una mala gestión. Presentar ejemplos sobre grandes ciberataques debido a vulnerabilidades en el sistema. Evaluación de contenidos + Incentivo para las mejores calificaciones.
Febrero	Importancia de los datos sensibles en una organización. El rol de la infraestructura, proveedores y los trabajadores en la seguridad de un sistema. Evaluación de contenidos + Incentivo para las mejores calificaciones.
Marzo	Tipos de ciberataques y como identificarlos. Recomendaciones y planes de acción frente a un ciberataque u otro incidente. Evaluación de contenidos + Incentivo para las mejores calificaciones.
Abril	Importancia de una autenticación segura en el sistema. Buenas prácticas para una codificación segura. Evaluación de contenidos + Incentivo para las mejores clasificaciones.
Mayo	Fallas de Inyección (tales como SQL o LDAP) y métodos de prevención. Pérdida de autenticación y gestión de sesiones Evaluación de contenidos + Incentivo para las mejores calificaciones.
Junio	Cross-Site Scripting (XSS) Evaluación de contenidos + Incentivo para las mejores calificaciones.

Fuente: Elaboración Propia

Tabla 26 – Plan de concientización (Continuación)

Actividades	
Julio	Referencia directa e insegura a objetos internos. Evaluación de contenidos + Incentivo para las mejores calificaciones.
Agosto	Mala configuración de seguridad en el sistema Evaluación de contenidos + Incentivo para las mejores calificaciones.
Septiembre	Vulnerabilidades por insuficiencia de monitoreo y registro en el sistema. Evaluación de contenidos + Incentivo para las mejores calificaciones.
Octubre	Exposición de datos sensibles en aplicaciones web. Evaluación de contenidos + Incentivo para las mejores calificaciones.
Noviembre	XML External Entity, en que consiste, como detectarlo y como prevenirlo. Evaluación de contenidos + Incentivos para las mejores calificaciones.
Diciembre	La deserialización insegura Evaluación de contenidos + Incentivos para las mejores calificaciones

Fuente: Elaboración Propia

A3. ISO 27001/2

Tabla 27 – Controles de Seguridad de la información ISO 27001/2

Anexo A de referencia	Título de control	Descripción del control
A.5	Políticas de seguridad de la Información	
A.5.1	Orientación de la dirección para la seguridad de la información	Proporcionar orientación de la dirección de la seguridad de la información según los requisitos del negocio y leyes pertinentes.
A.5.1.1	Documentación de política de la seguridad de la información	La administración debe aprobar, publicar y comunicar a todos los empleados internos o externos el documento de la política de seguridad de la información.
A.5.1.2	Revisión de las políticas de seguridad de la información	Se debe revisar periódicamente las políticas de seguridad de la información, o si se producen cambios significativos para asegurar su conveniencia, eficacia y suficiencia.
A.6	Organización de la seguridad de la información	
A.6.1	Organización interna	Se debe establecer un marco de trabajo de la dirección para controlar la implementación y funcionamiento de la seguridad de la información en la organización.
A.6.1.1	Roles y responsabilidades de la seguridad de la información	Se deben definir y gestionar correctamente las responsabilidades asociadas a la seguridad de la información.
A.6.1.2	Coordinación de roles de seguridad de la información	Se deben separar las funciones de la seguridad de información y coordinarlas con distintos roles para reducir el uso inadecuado de los activos de la organización no autorizados.
A.6.1.3	Comunicación con las autoridades	Se debe mantener la comunicación y coordinación con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especiales	Se debe mantener el contacto apropiado con los grupos especiales de interés, foros especializados en seguridad o asociaciones de profesionales especializados en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	Se debe abordar la seguridad de la información en cualquier tipo de proyecto.
A.6.2	Gestión de dispositivos móviles y trabajo remoto	Garantizar la seguridad en el trabajo remoto y el uso de dispositivos móviles.
A.6.2.1	Política de dispositivos móviles	Se debe adoptar una política de seguridad para gestionar los riegos en el uso de dispositivos móviles.
A.6.1.4	Contacto con grupos de interés especiales	Se debe mantener el contacto apropiado con los grupos especiales de interés, foros especializados en seguridad o asociaciones de profesionales especializados en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	Se debe abordar la seguridad de la información en cualquier tipo de proyecto.

Fuente: (ISO27000, 2017)

Tabla 26 – Controles de Seguridad de la información ISO 27001/2 (Continuación)

Anexo A de referencia	Título de control	Descripción del control
A.6.2	Gestión de dispositivos móviles y trabajo remoto	Garantizar la seguridad en el trabajo remoto y el uso de dispositivos móviles.
A.6.2.1	Política de dispositivos móviles	Se debe adoptar una política de seguridad para gestionar los riegos en el uso de dispositivos móviles.
A.6.2.2	Política de trabajo remoto	Se debe adoptar una política de seguridad para proteger la información a la que se accede, procesa o almacena en un trabajo remoto.
A.7	Recursos humanos de la seguridad de la información	
A.7.1	Previo al empleo	Asegurar que los empleados entiendan sus responsabilidades en la organización, y que sean aptos para los roles considerados
A.7.1.1	Selección	Se debe verificar antecedentes en todos los candidatos con relación a las leyes, regulaciones en proporción a los requisitos del negocio.
A.7.1.2	Términos y condiciones laborales	Los acuerdos entre empleados y contratistas deben indicar claramente las responsabilidades de estos y de la organización sobre la seguridad de la información.
A.7.2	Durante el empleo	Se debe asegurar que los empleados y contratistas estén en conocimiento y cumplan con sus responsabilidades asociadas a la seguridad de la información.
A.7.2.1	Responsabilidades de la dirección	La dirección debe solicitar a los empleados que apliquen la seguridad de la información de acuerdo con las políticas establecidas por la organización.
A.7.2.2	Concientización y formación en la seguridad de la información	Los empleados de la organización deben ser concientizados y actualizados regularmente en las políticas y procedimientos organizacionales relacionados a su función laboral.
A.7.3	Desvinculación y cambio de empleo	Se debe proteger los intereses de la organización en caso de desvinculación de un empleado.
A.7.3.1	Responsabilidades en la desvinculación o cambio de empleo	Se deben definir y comunicar las responsabilidades de la seguridad de la información que siguen en vigor después de la desvinculación laboral.
A.8	Administración de activos	
A.8.1	Responsabilidad de activos	Identificar y definir las responsabilidades sobre la protección de los activos de la organización.
A.8.1.1	Inventario de activos	Los activos relacionados con almacenamiento y procesamiento de información deben ser identificados, mantenidos y se deben realizar inventarios de estos.
A.8.1.2	Propiedad de los activos	Se deben identificar los propietarios de estos activos.
A.8.1.3	Uso aceptable de activos	Se deben definir, documentar e implementar las reglas para el uso de la información y los activos asociados a la información.
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de terceras partes deben devolver los activos pertenecientes a la organización en caso de finalización de la relación laboral.

Fuente: (ISO27000, 2017)

Tabla 26 – Controles de Seguridad de la información ISO 27001/2 (Continuación)

Anexo A de referencia	Título de control	Descripción del control
A.8.2	Clasificación de la información	Asegurar que la información recibe la protección adecuada de acuerdo con su importancia.
A.8.2.1	Clasificación de la información	La información debe ser clasificada según sus requisitos legales, valor, criticidad y sensibilidad frente a la divulgación o modificación sin previa autorización.
A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado de la información según el esquema de clasificación de la información adoptada por la organización.
A.8.2.3	Manejo de activos	Se deben desarrollar los procedimientos para el manejo de activos según el esquema de clasificación de información adoptado.
A.8.3	Manejo de los medios	Prevenir la divulgación, modificación o eliminación no autorizada de la información almacenada.
A.8.3.1	Gestión de los medios removibles	Se debe gestionar los medios removibles según el esquema de clasificación de la organización.
A.8.3.2	Eliminación de los medios	Se deben eliminar los medios de forma segura y sin peligro en caso de no necesitarse, utilizando procedimientos formales.
A.8.3.3	Transferencia física de medios	Los medios que contengan información se deben proteger contra acceso no autorizado o corrupción durante el transporte.
A.9	Control de acceso	
A.9.1	Requisitos de negocio para el control de acceso	Restringir el acceso a la información y a las instalaciones de procesamiento de información.
A.9.1.1	Política de control de a acceso	Se debe establecer, documentar y revisar una política de control de acceso basado en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Acceso a las redes y a los servicios de la red	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.
A.9.2	Gestión de acceso del usuario	Gestionar el acceso a usuarios registrados y restringir a los sin autorización a los sistemas y servicios.
A.9.2.1	Registro y eliminación de usuarios	Se debe implementar un proceso de registro y eliminación de usuarios.
A.9.2.2	Asignación de acceso de usuario	Debe existir un procedimiento para asignar o revocar los accesos a los diversos usuarios a los distintos sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiados	Se debe restringir y controlar la asignación y uso de accesos privilegiados.
A.9.2.4	Gestión de información secreta de autenticación de usuarios	Se debe controlar la asignación de información de autenticación mediante un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuario	Los propietarios de activos deben verificar los derechos de acceso de los usuarios periódicamente.

Fuente: (ISO27000, 2017)

Tabla 26 – Controles de Seguridad de la información ISO 27001/2 (Continuación)

Anexo A de referencia	Título de control	Descripción del control
A.9.2.6	Eliminación o ajuste de los derechos de acceso	Se deben retirar los derechos de acceso de los empleados y usuarios externos a la información, una vez que termine su acuerdo o relación laboral.
A.9.3	Responsabilidades del usuario	Asignar responsabilidad a los usuarios del cuidado de su información de autenticación.
A.9.3.1	Uso de la información de autenticación	Se debe exigir a los usuarios el cumplimiento de las prácticas de la organización en el uso de la información de autenticación.
A.9.4	Control de acceso al sistema y aplicaciones	Evitar el acceso sin autorización al sistema y aplicaciones.
A.9.4.1	Restricción de acceso a la información	Se debe restringir el acceso a la información y a las aplicaciones con la política de control de acceso.
A.9.4.2	Procedimientos de inicio de sesión seguro	Cuando la política de control lo exija, se debe asignar un procedimiento de inicio de sesión seguro al acceso de los sistemas y aplicaciones.
A.9.4.4	Uso de programas utilitarios privilegiados	Se debe controlar y restringir el uso de programas utilitarios que pueden ser capaz de anular el sistema y controles de aplicación.
A.9.4.5	Control de acceso al código fuente de los programas	Se debe restringir el acceso del código fuente de los diversos programas.
A.10	Criptografía	
A.10.1	Controles criptográficos	Se debe asegurar el uso adecuado y eficaz de criptografía, para así proteger la confidencialidad, autenticidad e integridad de la información.
A.10.1.1	Política sobre uso de controles criptográficos	Se debe desarrollar una política sobre el uso de controles criptográficos para proteger la información.
A.10.1.2	Gestión de claves	Se debe desarrollar una política sobre el uso, protección y vida útil de las claves criptográficas.
A.11	Seguridad física y ambiental	
A.11.1	Áreas seguras	Evitar accesos físicos no autorizados o daños en las instalaciones de procesamiento y almacenamiento de la información.
A.11.1.2	Controles de acceso físico	Las áreas seguras deben estar protegidas por controles de entradas que aseguren el acceso solo a personal autorizado.
A.11.1.3	Seguridad de oficinas, salas e instalaciones	Se debe diseñar y aplicar la seguridad física en las distintas instalaciones de la organización.
A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar la protección física contra daños por desastres naturales u otros accidentes.
A.11.1.5	Trabajo en áreas seguras	Se debe diseñar procedimientos para trabajar en lugares seguros.
A.11.1.6	Áreas de entrega y carga	Se debe controlar los accesos en áreas de entrega, carga y otros puntos, y si es posible, aislarlas de las instalaciones de procesamiento de información para evitar posibles accesos no autorizados.
A.11.2	Equipamiento	Se debe prevenir perdidas y daños de los activos, así como interrupción la interrupción de actividades en la organización.

Fuente: (ISO27000, 2017)

Tabla 26 – Controles de Seguridad de la información ISO 27001/2 (Continuación)

Anexo A de referencia	Título de control	Descripción del control
A.11.2.1	Ubicación y protección del equipamiento	El equipo se debe ubicar y proteger para reducir los riegos por accesos no autorizados y peligros ambientales.
A.11.2.2	Elementos de soporte	Se debe proteger el equipamiento contra fallas en el suministro de energía u otras interrupciones.
A.11.2.3	Seguridad en cableado	Se debe proteger el cableado de energía y de datos contra intercepción, interferencia o daños.
A.11.2.4	Mantenimiento del equipamiento	El equipamiento debe recibir el mantenimiento adecuado para asegurar su disponibilidad e integridad.
A.11.2.5	Retiro de activos	El equipamiento, información o software, no deben ser retirado de la organización sin previa autorización.
A.11.2.6	Seguridad del equipamiento y activos fuera de las instalaciones	Se deben asegurar los activos fuera de las instalaciones, considerando los riesgos de trabajar fuera de la organización.
A.11.2.7	Seguridad en la reutilización o descarte de equipos	Se debe asegurar que los datos sensibles y software licenciados se hayan removido o sobrescrito como medida de seguridad previo a la reutilización de equipos.
A.11.2.8	Equipo de usuario desatendido	Los usuarios se deben asegurar de la protección adecuada de los equipos desatendidos.
A.11.2.9	Política de escritorios y pantallas limpias	Se debe adoptar una política de escritorio limpio de papeles y medios de almacenamientos removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.
A.12	Seguridad de las operaciones	
A.12.1	Procedimientos operacionales y responsabilidades	Asegurar correcta operación y segura de las áreas de procesamiento de información.
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación deben estar documentados y a disposición para el que los necesite.
A.12.1.2	Gestión de cambios	Se deben controlar los cambios a la organización, el negocio, instalación de procesamiento de datos y cualquier otro sistema que afecte a la seguridad de la información.
A.12.1.3	Gestión de la capacidad	Se debe controlar el uso de recursos y se debe proyectar los futuros requisitos de capacidad para asegurar el desempeño del sistema.
A.12.1.4	Separación del ambiente de desarrollo, prueba y operaciones.	Los ambientes de desarrollo, prueba y operaciones deben estar separados para evitar accesos no autorizados o futuros cambios en el ambiente de estos.
A.12.2	Protección contra código malicioso	Asegurar que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra código malicioso	Se deben implantar controles de detección, recuperación y prevención, junto con concientización a los usuarios, para protegerse de los códigos maliciosos.

Fuente: (ISO27000, 2017)

Tabla 26 – Controles de Seguridad de la información ISO 27001/2 (Continuación)

Anexo A de referencia	Título de control	Descripción del control
A.12.3	Respaldo	Protegerse frente a una pérdida de datos.
A.12.4.4	Sincronización de relojes	La hora de los sistemas de procesamiento de información deben estar sincronizadas desde una única fuente.
A.12.5	Control de software de operación	Asegurar la integridad de los sistemas operacionales.
A.12.5.1	Instalación de software en sistemas operacionales.	Se deben crear procedimientos para controlar la instalación de software en los sistemas operacionales.
A.12.6	Gestión de la vulnerabilidad técnica	Evitar explotación de vulnerabilidades técnicas.
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener de manera oportuna la información de las vulnerabilidades técnicas de los sistemas de información usados, evaluar la exposición de la organización frente a estas y tomar las medidas apropiadas para abordar estos riesgos.
A.12.6.2	Restricciones en la instalación de software	Se deben establecer las reglas para regir la instalación de software por parte de los usuarios.
A.12.7	Consideraciones de las auditorías de los sistemas de información	Minimizar el impacto de las auditorías en los sistemas operacionales.
A.12.7.1	Controles de auditoría de los sistemas de información	Las auditorias que involucren verificación de los sistemas operacionales deben ser previamente planificados cuidadosamente para minimizar el riesgo de interrupciones en los procesos de negocio.
A.13	Seguridad de las comunicaciones	
A.13.1	Gestión de la seguridad de red	Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.
A.13.1.1	Controles de red	Las redes se deben gestionar y controlar para resguardar la información en los sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	Se deben identificar e incluir en los acuerdos de servicios de red todos los mecanismos de seguridad, niveles de servicios y requisitos de gestión de los servicios de red, ya que estos son prestados dentro de la organización o por terceros.
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes.
A.13.2	Transferencia de información	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
A.13.2.1	Políticas y procedimientos de intercambio de información	Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.

Fuente: (ISO27000, 2017)

Tabla 26 – Controles de Seguridad de la información ISO 27001/2 (Continuación)

Anexo A de referencia	Título de control	Descripción del control
A.13.2.2	Acuerdos de intercambio	Los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	Se debería proteger adecuadamente la información referida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad y secreto	Se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información
A.14	Adquisición, desarrollo y mantenimiento del sistema	
A.14.1	Requisitos de seguridad de los sistemas de información	Asegurar que la seguridad de la información es parte fundamental de los sistemas de información en todo el ciclo, incluido para los que proporcionan servicios en redes públicas.
A.14.1.1	Análisis y especificación de los requisitos de seguridad	Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	La información de los servicios de aplicación que pasan a través de redes públicas se debería proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.
A.14.1.3	Protección de las transacciones por redes telemáticas	La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.
A.14.2	Seguridad en procesos de desarrollo y soporte	Asegurar la integración de la seguridad de la información dentro del ciclo de desarrollo de los sistemas de información.
A.14.2.1	Política de desarrollo seguro	Las reglas para el desarrollo de software y sistemas deben ser establecidas y aplicadas a los desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambios del sistema	Los cambios a los sistemas dentro de ciclo de desarrollo deben ser controlados mediante un control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación	En caso de cambio de las plataformas de operación se debe poner a prueba las aplicaciones críticas del negocio para asegurar que no afecten en la operación o en la seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Se debe reducir las modificaciones a los paquetes de software solo a cambios estrictamente necesarios.
A.14.2.5	Principios de ingeniería de sistema seguro	Se debe establecer, documentar, mantener y aplicar los principios para los sistemas seguros de ingeniería para cualquier esfuerzo de implementación del sistema de información.
A.14.2.6	Entorno de desarrollo seguro	Se debe establecer y proteger los entornos de desarrollo seguro apropiadamente, para todo el ciclo de desarrollo del sistema

Fuente: (ISO27000, 2017)

Tabla 26 – Controles de Seguridad de la información ISO 27001/2 (Continuación)

Anexo A de referencia	Título de control	Descripción del control
A.14.2.7	Desarrollo mercerizado	La organización debería supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.
A.14.2.8	Prueba de seguridad del sistema	Durante el desarrollo se deben realizar pruebas de funcionalidad de seguridad.
A.14.2.9	Prueba de aprobación del sistema	Se deben definir las pruebas de aceptación y criterios pertinentes para los nuevos sistemas de información u actualizaciones de estos.
A.14.3	Datos de prueba	Proteger los datos usados para pruebas.
A.14.3.1	Protección de datos de prueba	Se deben seleccionar, proteger y controlar rigurosamente los datos de prueba.
A.15	Relaciones con el proveedor	
A.15.1	Seguridad de la información en las relaciones con el proveedor	Se debe asegurar la protección de los activos que tiene acceso los proveedores.
A.15.1.1	Política de seguridad de la información para las relaciones con el proveedor	Se deben acordar y documentar, junto con el proveedor, los requisitos de la seguridad de la información para mitigar los riesgos asociados al acceso del proveedor a los activos de la organización.
A.15.1.2	Abordar la seguridad dentro de los acuerdos del proveedor	Los requisitos de seguridad de la información deben ser definidos y acordado con los proveedores que puedan acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la organización.
A.15.1.3	Cadena de suministro de tecnologías de información y comunicaciones	Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociado a los servicios de la tecnología de la información, comunicaciones y la cadena de suministro del producto.
A.15.2	Gestión de entrega del servicio del proveedor	Mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos del proveedor.
A.15.2.1	Supervisión y revisión de los servicios del proveedor	Se debe supervisar, revisar y auditar la entrega del servicio del proveedor.
A.15.2.2	Gestión de cambios a los servicios del proveedor	Se deben gestionar los cambios al suministro de los servicios por parte de los proveedores, incluido al mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles al considerar la criticidad de la información del negocio, los sistemas y procesos involucrados y la reevaluación de los riegos.
A.16	Gestión de incidentes de seguridad de la información	
A.16.1	Gestión de incidentes de seguridad de la información y mejoras	Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Fuente: (ISO27000, 2017)

Tabla 26 – Controles de Seguridad de la información ISO 27001/2 (Continuación)

Anexo A de referencia	Título de control	Descripción del control
A.16.1.1	Responsabilidades y procedimientos	Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información.
A.16.1.2	Informe de eventos de seguridad de la información	Se deben informar rápidamente los eventos de seguridad de la información mediante canales de gestión apropiados.
A.16.1.3	Informe de las debilidades de seguridad de la información	Se debe requerir que los empleados y contratistas que usen los sistemas y servicios de información de la organización observen e informen cualquier debilidad en la seguridad de la información en los sistemas o servicios observada o que se sospeche.
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Los eventos de seguridad de la información se deben evaluar y decidir si serán clasificados como incidentes de seguridad de la información.
A.16.1.5	Respuesta ante incidentes de la seguridad de la información	Los incidentes de seguridad deben ser atendido según los procedimientos ya documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Se debe utilizar el conocimiento para analizar y resolver los incidentes de seguridad de la información para reducir la probabilidad o impacto a futuro de estos.
A.16.1.7	Recolección de evidencia	Se debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información, para tenerlos como evidencia.
A.17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	
A.17.1	Continuidad de la seguridad de la información	Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad del negocio de la organización.
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de gestión de la seguridad de la información en situaciones adversas como crisis o desastres.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Se debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar periódicamente los controles de continuidad de la seguridad de la información definidos e implementados para asegurar la validez y eficacia durante situaciones adversas
A.17.2	Redundancias	Asegurar la disponibilidad de las instalaciones de procesamiento de la información.
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.
A.18	Cumplimiento	

Fuente: (ISO27000, 2017)

Tabla 26 – Controles de Seguridad de la información ISO 27001/2 (Continuación)

Anexo A de referencia	Título de control	Descripción del control
A.18.1	Cumplimiento con los requisitos legales y contractuales	Evitar incumplimientos de la obligaciones legales, estatutarias, regulatorias o contractuales relacionados con la seguridad de la información y todos los requisitos de seguridad.
A.18.1.1	Identificación de la legislación vigente y los requisitos contractuales	Se deberían identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.
A.18.1.2	Derechos de propiedad intelectual	Se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software originales.
A.18.1.3	Protección de los registros	Los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.
A.18.1.4	Privacidad y protección de la información de identificación personal	Se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.
A.18.1.5	Regulación de los controles criptográficos	Se deberían utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.
A.18.2	Revisiones de seguridad de la información	Asegurar la implementación de la seguridad de la información y que funcione de acuerdo con las políticas y procedimientos de la organización.
A.18.2.1	Revisión independiente de la seguridad de la información	Se debería revisar el enfoque de la organización para la implementación los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.
A.18.2.3	Verificación del cumplimiento técnico.	Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.

Fuente: (ISO27000, 2017)

A4. PCI-DSS V3.2

Tabla 28 - Requisitos y controles de seguridad de la información PCI-DSS v3.2

Requisitos de las PCI DSS
1.1 Establezca e implemente normas de configuración para firewalls y routers que incluyan lo siguiente:
1.1 Inspeccione las normas de configuración de firewalls y routers y otros documentos especificados a continuación para verificar el cumplimiento e implementación de las normas.
1.1.1 Un proceso formal para aprobar y probar todos los cambios y las conexiones de red en la configuración de los firewalls y los routers
1.1.1.a Revise los procedimientos documentados para corroborar que existe un proceso formal para aprobar y probar lo siguiente: Conexiones de red Cambios en las configuraciones de firewalls y routers
1.1.1.b Para obtener una muestra de las conexiones de red, entreviste al personal responsable y revise los registros para verificar que se hayan aprobado y probado las conexiones de red.
1.1.1.c Identifique una muestra de los cambios reales realizados en las configuraciones de firewalls y routers, compárela con los registros de cambio y entreviste al personal responsable para verificar que los cambios se hayan probado y aprobado.
1.1.2 Diagrama de red actual que identifica todas las conexiones entre el entorno de datos de titulares de tarjetas y otras redes, incluso cualquier red inalámbrica.
1.1.2.a Revise los diagramas y observe las configuraciones de red para verificar que exista un diagrama de red actual que documente todas las conexiones con los datos de los titulares de tarjetas, incluso las redes inalámbricas.
1.1.2.b Entreviste al personal responsable para verificar que el diagrama esté actualizado.
1.1.3 El diagrama actual que muestra todos los flujos de datos de titulares de tarjetas entre los sistemas y las redes.
1.1.3 Revise el diagrama de flujo de datos y entreviste al personal para verificar lo siguiente en el diagrama: Muestra los flujos de datos de titulares de tarjetas entre los sistemas y las redes. Se mantiene al día y está actualizado según los cambios implementados en el entorno.
1.1.4 Requisitos para tener un firewall en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna.
1.1.4.a Revise las normas de configuración de firewalls y controle que incluyan los requisitos para tener un firewall en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna.
1.1.4.b Verifique que el diagrama de red actual concuerde con las normas de configuración de firewalls.
1.1.4.c Revise las configuraciones de red para verificar que haya un firewall en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna, de acuerdo con las normas de configuración documentadas y los diagramas de red.
1.1.5 Descripción de grupos, funciones y responsabilidades para la administración de los componentes de la red.
1.1.5.a Verifique que las normas de configuración de firewalls y routers incluyan la descripción de los grupos, las funciones y las responsabilidades para la administración de los componentes de la red.
1.1.5.b Entreviste al personal responsable de administrar los componentes de la red para confirmar que las funciones y las responsabilidades se hayan asignado según lo documentando.

Fuente: (PCI Security Standards Council, 2016)

Tabla 29 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
1.1.6 Documentación y justificación de negocio para el uso de todos los servicios, protocolos y puertos permitidos, incluida la documentación de las funciones de seguridad implementadas en aquellos protocolos que se consideran inseguros. **1.1.6.a** Verifique que las normas de configuración de firewalls y routers incluyan una lista documentada de todos los servicios, protocolos y puertos, incluida la justificación comercial y la aprobación para cada una. **1.1.6.b** Identifique los servicios, protocolos y puertos inseguros permitidos y verifique que se hayan documentado las funciones de seguridad de cada servicio. **1.1.6.c** Revise las configuraciones de firewalls y routers para verificar que se hayan implementado las funciones de seguridad para cada servicio, protocolo y puerto inseguros.
1.1.7 Requisito de la revisión de las normas de firewalls y routers, al menos, cada seis meses. **1.1.7.a** Verifique que las normas de configuración de firewalls y routers soliciten la revisión de las reglas, al menos, cada seis meses. **1.1.7.b** Examine la documentación relacionada con las revisiones de las reglas y entreviste al personal responsable para verificar si las reglas se revisan, al menos, cada seis meses.
1.2 Desarrolle configuraciones para firewalls y routers que restrinjan las conexiones entre redes no confiables y cualquier componente del sistema en el entorno de los datos de titulares de tarjetas. **1.2** Revise las configuraciones de firewalls y routers y realice las siguientes acciones para verificar que se restringen las conexiones entre redes no confiables y todo componente del sistema en el entorno de datos de titulares de tarjetas:
1.2.1 Restrinja el tráfico entrante y saliente a la cantidad necesaria para el entorno de datos de los titulares de tarjetas y niegue específicamente el tráfico restante. **1.2.1.a** Revise las normas de configuración de firewalls y routers para verificar que identifican el tráfico entrante y saliente necesario para el entorno de datos de titulares de tarjetas. **1.2.1.b** Revise las configuraciones de firewalls y routers para verificar que el tráfico entrante y saliente esté restringido a la cantidad necesaria para el entorno de datos de titulares de tarjetas. **1.2.1.c** Revise las configuraciones de firewalls y routers para verificar que todo tráfico entrante y saliente se niegue de manera específica, por ejemplo, mediante una declaración explícita “negar todos” o una negación implícita después de una declaración de permiso.
1.2.2 Asegure y sincronice los archivos de configuración de routers. **1.2.2.a** Revise los archivos de configuración del router para verificar que están protegidos contra el acceso no autorizado. **1.2.2.b** Revise las configuraciones del router y verifique que estén sincronizadas, por ejemplo, que la configuración en ejecución (o activa) coincida con la configuración de inicio (que se usa cuando la máquina se reinicia).
1.2.3 Instale firewalls de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta y configure estos firewalls para negar o, si el tráfico es necesario para fines comerciales, permitir solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta. **1.2.3.a** Revise las configuraciones de firewalls y routers, y verifique que se hayan instalado firewalls de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta. **1.2.3.b** Verifique que los firewalls nieguen o, si el tráfico es necesario para fines comerciales, permitan solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta.
1.3 Prohíba el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas. **1.3** Revise las configuraciones de firewalls y routers, que incluye, entro otros, el router de estrangulamiento de Internet, el router DMZ y el firewall, el segmento de titulares de tarjetas de DMZ, el router de perímetro y el segmento de la red interna del titular de la tarjeta, y realice lo siguiente a fin de determinar que no exista un acceso directo entre la Internet y los componentes del sistema en el segmento de red interna de los titulares de tarjeta:

Fuente: (PCI Security Standards Council, 2016)

Tabla 30 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
1.3.1 Implemente una DMZ (zona desmilitarizada) para limitar el tráfico entrante solo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado. **1.3.1** Revise las configuraciones de firewalls y routers, y verifique que se haya implementado una DMZ (zona desmilitarizada) para limitar el tráfico entrante solo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado.
1.3.2 Restrinja el tráfico entrante de Internet a las direcciones IP dentro de la DMZ. **1.3.2** Revise las configuraciones de firewalls y routers, y verifique que se restrinja el tráfico entrante de Internet a las direcciones IP dentro de la DMZ.
1.3.3 Implementar medidas anti-suplantación para detectar y bloquear direcciones IP manipuladas a fin de que no ingresen en la red. (Por ejemplo, bloquear el tráfico proveniente de Internet con una dirección de fuente interna). **1.3.3** Revise las configuraciones de firewalls y routers, y verifique que se hayan implementado medidas contra la suplantación, por ejemplo, las direcciones internas no se pueden transferir de Internet a la DMZ.
1.3.4 No permita que el tráfico saliente no autorizado proveniente del entorno de datos del titular de la tarjeta ingrese en Internet. **1.3.4** Revise las configuraciones de firewalls y routers, y verifique que el tráfico saliente proveniente del entorno de datos del titular de la tarjeta a Internet esté explícitamente autorizado.
1.3.5 Solo permita conexiones "establecidas" en la red. **1.3.5** Revise las configuraciones de firewalls y routers para verificar que los firewalls permiten solo conexiones establecidas en la red interna y que niegan cualquier conexión entrante que no está asociada con una sesión previamente establecida.
1.3.6 Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna segregada desde una DMZ (zona desmilitarizada) y otras redes no confiables. **1.3.6** Revise las configuraciones de firewalls y routers, y verifique que los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) se encuentren en una zona de red interna segregada desde una DMZ (zona desmilitarizada) y otras redes no confiables.
1.3.7 No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas. Por ejemplo: • *Traducción de Dirección de Red (NAT)* • *Ubicación de los servidores que contengan datos del titular de la tarjeta detrás de los servidores proxy/firewalls.* • *Eliminación o filtrado de anuncios de enrutamiento para redes privadas que emplean direcciones registradas* • *Uso interno del espacio de direcciones RFC1918 en lugar de direcciones registradas.* **1.3.7.a** Revise las configuraciones de firewalls y routers, y verifique que se hayan implementado métodos para prevenir la divulgación de direcciones IP privadas e información de enrutamiento desde redes internas a Internet. **1.3.7.b** Entreviste al personal, revise la documentación y verifique que no se autorice la divulgación de ninguna dirección IP privada ni de información de enrutamiento a entidades externas.

Fuente: (PCI Security Standards Council, 2016)

Tabla 31 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
1.4 Instale software de firewall personal o una funcionalidad equivalente en todos los dispositivos móviles (de propiedad de la compañía y/o de los trabajadores) que tengan conexión a Internet cuando están fuera de la red (por ejemplo, computadoras portátiles que usan los trabajadores), y que también se usan para acceder al CDE. Las configuraciones de firewall (o equivalente) incluyen: • Se definen los ajustes específicos de configuración. • El firewall personal (o funcionalidad equivalente) está en ejecución activa. • El firewall personal (o una funcionalidad equivalente) no es alterable por los usuarios de los dispositivos informáticos portátiles. **1.4.a** Revise las políticas y las normas de configuración para verificar lo siguiente: Se debe incluir software de firewall personal o una funcionalidad equivalente en todos los dispositivos móviles (de propiedad de la compañía y/o de los trabajadores) que tengan conexión a Internet cuando están fuera de la red (por ejemplo, computadoras portátiles que usan los trabajadores), y que también se usen para acceder al CDE. • Los parámetros específicos de configuración se definen para cada software de firewall personal (o funcionalidad equivalente). • El firewall personal (o una funcionalidad equivalente) está configurado para ejecutarse de forma activa. • El firewall personal (o una funcionalidad equivalente) está configurado para no ser alterado por los usuarios de los dispositivos informáticos portátiles. **1.4.b** Inspeccione una muestra de dispositivos móviles de propiedad de la empresa y/o de los trabajadores para verificar que: • El firewall personal (o funcionalidad equivalente) está instalado y configurado de conformidad con los parámetros de configuración específicos de la empresa. • El firewall personal (o funcionalidad equivalente) está en ejecución activa. • El firewall personal (o una funcionalidad equivalente) no es alterable por los usuarios de los dispositivos informáticos portátiles.
1.5 Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los firewalls estén documentados, implementados y que sean de conocimiento para todas las partes afectadas. **1.5** Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos para administrar los firewalls cumplan con lo siguiente: • Estén documentados, • Estén en uso, y • Sean de conocimiento para todas las partes afectadas.

Fuente: (PCI Security Standards Council, 2016)

Tabla 32 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
2.1 Siempre cambie los valores predeterminados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias **antes** de instalar un sistema en la red. Esto rige para TODAS las contraseñas predeterminadas, por ejemplo, entre otras, las utilizadas por los sistemas operativos, los software que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, *los terminales de POS (*puntos de venta*)*, las aplicación de pago, las cadenas comunitarias de SNMP (protocolo simple de administración de red), etc. **2.1.a** Escoja una muestra de los componentes del sistema e intente acceder a los dispositivos y aplicaciones (con la ayuda del administrador del sistema) con las cuentas y contraseñas predeterminadas por el proveedor y verifique que se hayan cambiado TODAS las contraseñas predeterminadas (incluso las de los sistemas operativos, los software que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales de POS [puntos de ventas], las cadenas comunitarias de SNMP [protocolo simple de administración de red]). **2.1.b** Para la muestra de los componentes del sistema, verifique que todas las cuentas predeterminadas innecesarias (incluso las cuentas que usan los sistemas operativos, los softwares de seguridad, las aplicaciones, los sistemas, los terminales de POS [puntos de ventas], SNMP [protocolo simple de administración de red], etc.) se hayan eliminado o estén deshabilitadas. **2.1.1.c** Revise la documentación proporcionada por el proveedor, inicie sesión en los dispositivos inalámbricos con la ayuda del administrador del sistema y verifique lo siguiente: • No se usan las cadenas comunitarias SNMP (protocolo simple de administración de red) predeterminadas. • No se usan las contraseñas/frases predeterminadas de los puntos de acceso. **2.1.1.d** Revise la documentación proporcionada por el proveedor, observe los parámetros de la configuración inalámbrica y verifique que el firmware de los dispositivos inalámbricos se actualice a fin de admitir el cifrado sólido para lo siguiente: • Autenticación en redes inalámbricas. Transmisión en redes inalámbricas. **2.1.1.e** Revise la documentación proporcionada por el proveedor, observe los parámetros de la configuración inalámbrica y verifique que se hayan cambiado los otros valores predeterminados proporcionados por los proveedores relacionados con la seguridad de los sistemas inalámbricos, según corresponda.

Fuente: (PCI Security Standards Council, 2016)

Tabla 33 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
2.2 Desarrolle normas de configuración para todos los componentes de sistemas. Asegúrese de que estas normas contemplen todas las vulnerabilidades de seguridad conocidas y que concuerden con las normas de alta seguridad de sistema aceptadas en la industria. Entre las fuentes de normas de alta seguridad aceptadas en la industria, se pueden incluir, a modo de ejemplo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • Institute National Institute of Standards Technology (NIST). **2.2.a** Examine las normas de configuración de sistemas de la organización correspondientes a todos los tipos de componentes de sistemas y verifique que las normas de configuración de sistemas concuerden con las normas de alta seguridad aceptadas en la industria. **2.2.b** Revise las políticas, entreviste al personal y verifique que las normas de configuración de sistemas se actualicen a medida que se identifiquen nuevas vulnerabilidades, tal como se define en el Requisito 6.1. **2.2.c** Revise las políticas, entreviste al personal y verifique que se apliquen las normas de configuración de sistemas al configurar y comprobar que se instalaron nuevos sistemas antes de instalar un sistema en la red. **2.2.d** Verifique que las normas de configuración de sistemas incluyan los siguientes procedimientos para todos los tipos de componentes del sistema: • Cambiar los valores predeterminados de los proveedores y eliminar las cuentas predeterminadas innecesarias. • Implementar solo una función principal por servidor a fin de evitar que coexistan funciones que requieran diferentes niveles de seguridad en el mismo servidor. • Habilitar solo los servicios, protocolos, daemons, etc., necesarios, según lo requiera la función del sistema. • Implementar funciones de seguridad adicionales para los servicios, protocolos o daemons requeridos que no se consideren seguros. • Configurar los parámetros de seguridad del sistema para evitar el uso indebido. • Eliminar todas las funcionalidades innecesarias, como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios.
2.2.1 Implemente sólo una función principal por servidor a fin de evitar que coexistan funciones que requieren diferentes niveles de seguridad en el mismo servidor. (Por ejemplo, los servidores web, servidores de base de datos y DNS se deben implementar en servidores separados). ***Nota:*** *Cuando se utilicen tecnologías de virtualización, implemente solo una función principal por componente de sistema virtual.* **2.2.1.a** Seleccione una muestra de los componentes del sistema, inspeccione las configuraciones del sistema y verifique que se haya implementado solo una función principal en cada servidor. **2.2.1.b** Si se utilizan tecnologías de virtualización, inspeccione las configuraciones del sistema y verifique que se haya implementado una sola función principal por componente de sistema o dispositivo virtual.
2.2.2 Habilite solo los servicios, protocolos y daemons, etc., necesarios, según lo requiera la función del sistema. **2.2.2.a** Seleccione una muestra de los componentes del sistema, inspeccione los servicios del sistema, daemons y protocolos habilitados y verifique que solo se habiliten los servicios o protocolos necesarios. **2.2.2.b** Identifique los servicios, daemons o protocolos habilitados que no sean seguros, entreviste al personal y verifique que estén configurados de conformidad con las normas de configuración documentadas.

Fuente: (PCI Security Standards Council, 2016)

Tabla 34 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
2.2.3 Implementar funciones de seguridad adicionales para los servicios, protocolos o daemons requeridos que no se consideren seguros. ***Nota:*** *Cuando se utiliza la SSL/TLS temprana, se debe completar los requisitos establecidos en el Anexo A2.* **2.2.3.a** Inspeccione los parámetros de configuración y verifique que las funciones de seguridad se hayan documentado e implementado en todos los servicios, daemons o protocolos no seguros. **2.2.3.b** Si se utiliza la SSL/TLS temprana, realice los procedimientos de prueba en el *Anexo A2: Requisitos adicionales de la PCI DSS para las entidades que utilizan SSL/TLS temprana.*
2.2.4 Configure los parámetros de seguridad del sistema para evitar el uso indebido. **2.2.4.a** Entreviste a los administradores del sistema o a los gerentes de seguridad para verificar que conocen las configuraciones comunes de parámetros de seguridad de los componentes del sistema. **2.2.4.b** Revise las normas de configuración de sistemas y verifique que incluyan los valores comunes de los parámetros de seguridad. **2.2.4.c** Seleccione una muestra de los componentes del sistema e inspeccione los parámetros de seguridad comunes para verificar que se hayan configurado correctamente, según las normas de configuración.
2.2.5 Elimine todas las funcionalidades innecesarias, como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios. **2.2.5.a** Seleccione una muestra de los componentes del sistema, inspeccione las configuraciones y verifique que se hayan eliminado todas las funcionalidades innecesarias (por ejemplo, secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos, etc.). **2.2.5.b**. Revise la documentación y los parámetros de seguridad, y verifique que las funciones habilitadas estén documentadas y admitan la configuración segura. **2.2.5.c**. Revise la documentación y los parámetros de seguridad, y verifique que solo la funcionalidad documentada esté presente en la muestra de componentes del sistema.
2.3 Cifre todo el acceso administrativo que no sea de consola utilizando un cifrado sólido. Nota: Cuando se utiliza la SSL/TLS temprana, se debe completar los requisitos establecidos en el Anexo A2. **2.3** Seleccione una muestra de los componentes del sistema y verifique que el acceso administrativo que no sea de consola se cifre al realizar lo siguiente: **2.3.a** Observe a un administrador mientras inicia sesión en cada sistema y revise las configuraciones de los sistemas a fin de controlar que se invoca un método sólido de cifrado antes de que se solicite la contraseña del administrador. **2.3.b** Revise los servicios y los archivos de parámetros en los sistemas a fin de determinar que Telnet y otros comandos de inicio de sesión remotos inseguros no están disponibles para acceso sin consola. **2.3.c** Observe a un administrador mientras inicia sesión en cada sistema y verifique que el acceso del administrador a cualquier interfaz de administración basada en la Web esté cifrado mediante una criptografía sólida. **2.3.d** Revise la documentación del proveedor y entreviste al personal a fin de controlar que se implemente una criptografía sólida para la tecnología usada de acuerdo con las mejores prácticas de la industria y las recomendaciones del proveedor. **2.3.e** Si se utiliza la SSL/TLS temprana, realice los procedimientos de prueba en el Anexo A2: Requisitos adicionales de la PCI DSS para las entidades que utilizan SSL/TLS temprana.
2.4 Lleve un inventario de los componentes del sistema que están dentro del alcance de las PCI DSS. **2.4.a** Revise el inventario del sistema para verificar que haya una lista de componentes del hardware y del software con una descripción de la función/uso de cada componente. **2.4.b** Entreviste al personal y verifique que el inventario esté actualizado.

Fuente: (PCI Security Standards Council, 2016)

Tabla 35 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
2.5 Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los parámetros predeterminados del proveedor y otros parámetros de seguridad estén documentados, implementados y que sean de conocimiento para todas las partes afectadas. **2.5** Revise la documentación, entreviste al personal y verifique que las políticas de seguridad y los procedimientos operativos para administrar los parámetros predeterminados del proveedor y otros parámetros de seguridad cumplen con lo siguiente: • Estén documentados, • Estén en uso, y • Sean de conocimiento para todas las partes afectadas.
2.6 Los proveedores de hosting compartido deben proteger el entorno y los datos del titular de la tarjeta que aloja la entidad. Estos proveedores deben cumplir requisitos específicos detallados en el Anexo A1: Requisitos adicionales de las DSS de la PCI para los proveedores de servicios de hosting. **2.6** Lleve a cabo los procedimientos de pruebas desde A.1.1 hasta A.1.4 que se describen en el Anexo A1: Requisitos adicionales de las PCI DSS para los proveedores de hosting compartido en lo que respecta a la evaluación de las PCI DSS de los proveedores de hosting compartido para verificar que estos proveedores protejan el entorno y los datos que alojan las entidades (comerciantes y proveedores de servicios).
3.1 Almacene la menor cantidad posible de datos del titular de la tarjeta implementando políticas, procedimientos y procesos de retención y eliminación de datos que incluyan, al menos, las siguientes opciones para el almacenamiento de CHD (datos del titular de la tarjeta): · Limitación del almacenamiento de datos y del tiempo de retención a la cantidad exigida por los requisitos legales, reglamentarios y del negocio · Requisitos de retención específicos para datos de titulares de tarjetas · Procesos para eliminar datos de manera cuando ya no se necesiten · Un proceso trimestral para identificar y eliminar, de manera segura, los datos del titular de la tarjeta almacenados que excedan la retención definida. **3.1.a** Revise las políticas, los procedimientos y los procesos de retención y eliminación de datos y verifique que incluyen lo siguiente para todo el almacenamiento de los datos del titular de la tarjeta (CHD): · Limitación del almacenamiento de datos y del tiempo de retención a la cantidad exigida por los requisitos legales, reglamentarios y del negocio. · Requisitos específicos para la retención de datos del titular de la tarjeta (por ejemplo, los datos del titular de la tarjeta se debe mantener durante X tiempo por Y razones de la empresa). · Eliminación segura de los datos del titular de la tarjeta cuando ya no son necesarios por motivos legales, reglamentarios o empresariales. · Un proceso trimestral para identificar y eliminar, de manera segura, los datos del titular de la tarjeta almacenados que excedan los requisitos de retención definidos. **3.1.b** Entreviste al personal y verifique lo siguiente: · Todos los lugares donde se almacenan los datos del titular de la tarjeta están incluidos en los procesos de retención y eliminación de datos. · Se implementa un proceso trimestral automático o manual para identificar y eliminar, de manera segura, los datos del titular de la tarjeta almacenados. · El proceso trimestral automático o manual se lleva a cabo en todas las ubicaciones de datos del titular de la tarjeta. **3.1.c** Para obtener una muestra de los componentes del sistema que almacenan datos del titular de la tarjeta: · Revise los archivos y los registros del sistema para verificar que los datos almacenados no superen los requisitos definidos en la política de retención de datos. · Observe el mecanismo de eliminación y verifique que los datos se eliminen de manera segura.

Fuente: (PCI Security Standards Council, 2016)

Tabla 36 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
3.2 No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). Si se reciben datos de autenticación confidenciales, convierta todos los datos en irrecuperables al finalizar el proceso de autorización. *Es posible que los emisores de tarjetas y las empresas que respaldan los servicios de emisión almacenen datos de autenticación confidenciales en los siguientes casos:* · Si existe una justificación de negocio. · Si los datos se almacenan de forma segura. Los datos confidenciales de autenticación incluyen los datos mencionados en los requisitos 3.2.1 a 3.2.3, establecidos a continuación: **3.2.a** En el caso de los emisores de tarjetas o las empresas que respaldan servicios de emisión y almacenan datos de autenticación confidenciales, revise las políticas y entreviste al personal para verificar que existe una justificación de negocio documentada para almacenar datos de autenticación confidenciales. **3.2.b** En el caso de los emisores de tarjetas o las empresas que respaldan servicios de emisión y almacenan datos de autenticación confidenciales, revise los almacenamientos de datos y la configuración del sistema para verificar que los datos de autenticación confidenciales estén protegidos. **3.2.c** En el caso de otras entidades, si se reciben datos de autenticación confidenciales, revise las políticas y los procedimientos, y revise la configuración del sistema a fin de verificar que los datos no se conservan después de la autorización. **3.2.d** En el caso de otras entidades, si se reciben datos de autenticación confidenciales, revise los procedimientos y analice los procesos de eliminación segura de datos a fin de verificar que los datos sean irrecuperables.
3.2.1 No almacene contenido completo de ninguna pista (de la banda magnética ubicada en el reverso de la tarjeta, datos equivalentes que están en un chip o en cualquier otro dispositivo) después de la autorización. Estos datos se denominan alternativamente, pista completa, pista, pista 1, pista 2 y datos de banda magnética. ***Nota:*** *En el transcurso normal de los negocios, es posible que se deban retener los siguientes elementos de datos de la banda magnética:* · *El nombre del titular de la tarjeta* · *Número de cuenta principal (PAN)* · *Fecha de vencimiento* · *Código de servicio* *Para minimizar el riesgo, almacene solamente los elementos de datos que sean necesarios para el negocio.* **3.2.1** En el caso de la muestra de componentes del sistema, revise las fuentes de datos, incluido, a modo de ejemplo, lo siguiente y verifique que el contenido completo de cualquier pista de la banda magnética en el reverso de la tarjeta o cualesquiera datos almacenados en un chip no se almacenen después de la autorización: · Datos de transacciones entrantes · Todos los registros (por ejemplo, transacciones, historiales, depuración, error) · Archivos de historial · Archivos de seguimiento · Esquemas de bases de datos · Contenidos de bases de datos

Fuente: (PCI Security Standards Council, 2016)

Tabla 37 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
3.2.2 No almacene el valor o código de validación de tarjetas (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de pago que se utiliza para verificar las transacciones de tarjetas ausentes) después de la autorización. **3.2.2** En el caso de la muestra de componentes del sistema, revise las fuentes de datos, incluido, a modo de ejemplo, lo siguiente y verifique que el código o el valor de verificación de la tarjeta de tres o de cuatro dígitos impreso en el anverso de la tarjeta o en el panel de firma (datos CVV2, CVC2, CID, CAV2) no se almacene después de la autorización: · Datos de transacciones entrantes · Todos los registros (por ejemplo, transacciones, historiales, depuración, error) · Archivos de historial · Archivos de seguimiento · Esquemas de bases de datos · Contenidos de bases de datos
3.2.3 Después de la autorización, no almacene el PIN (número de identificación personal) ni el bloqueo de PIN cifrado. **3.2.3** En el caso de la muestra de los componentes del sistema, revise las fuentes de datos, incluido, a modo de ejemplo, lo siguiente y verifique que los PIN y los bloqueos de PIN cifrados no se almacenen después de la autorización: · Datos de transacciones entrantes · Todos los registros (por ejemplo, transacciones, historiales, depuración, error) · Archivos de historial · Archivos de seguimiento · Esquemas de bases de datos · Contenidos de bases de datos
3.3 Enmascare el PAN (número de cuenta principal) cuando aparezca (los primeros seis o los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá), de modo que solo el personal con una necesidad comercial legítima pueda ver más que los primeros seis o los últimos cuatro dígitos del PAN. **3.3.a** Revise las políticas y los procedimientos escritos para ocultar las vistas de PAN (número de cuenta principal) para verificar lo siguiente: · Se documenta una lista de las funciones que necesitan acceso a más que los primeros seis o los últimos cuatro dígitos (incluye el PAN completo), junto con la necesidad empresarial legítima que justifique dicho acceso. · Se debe ocultar el PAN cuando aparezca para que solo el personal con una necesidad comercial legítima pueda ver más que los primeros seis y los últimos cuatro dígitos del PAN. · Todas las demás funciones que no estén específicamente autorizadas para ver el PAN completo, solo deben ver el PAN oculto. **3.3.b** Revise las configuraciones del sistema y verifique que las vistas del PAN (número de cuenta principal) estén disponibles solo para aquellos usuarios/funciones que tengan una necesidad comercial legítima y que el PAN (número de cuenta principal) esté oculto para el resto de las solicitudes. **3.3.c** Revise las vistas del PAN (por ejemplo, en la pantalla o en recibos en papel) a fin de controlar que los PAN se oculten cuando muestren los datos del titular de la tarjeta, y que solo aquellos con una necesidad empresarial legítima puedan ver más que los primeros seis o los últimos cuatro dígitos del PAN.

Fuente: (PCI Security Standards Council, 2016)

Tabla 38 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
3.4 Convierta el PAN (número de cuenta principal) en ilegible en cualquier lugar donde se almacene (incluidos los datos que se almacenen en medios digitales portátiles, en medios de copia de seguridad y en registros) utilizando cualquiera de los siguientes métodos: · Valores hash de una vía basados en criptografía sólida (el hash debe ser del PAN completo) · Truncamiento (los valores hash no se pueden usar para reemplazar el segmento truncado del PAN) · Tokens y ensambladores de índices (los ensambladores se deben almacenar de manera segura). · Criptografía sólida con procesos y procedimientos asociados para la administración de claves. **Nota:** Para una persona malintencionada sería relativamente fácil reconstruir el PAN original si tiene acceso tanto a la versión truncada como a la versión en valores hash de un PAN. Si el entorno de una entidad tiene versiones en valores hash y truncadas del mismo PAN, se deben implementar controles adicionales para asegurar que las versiones en valores hash y truncadas no se puedan correlacionar para reconstruir el PAN original.
3.4.a Revise la documentación sobre el sistema utilizado para proteger el PAN (número de cuenta principal), que incluye el proveedor, el tipo de sistema/proceso y los algoritmos de cifrado (si corresponde), y verifique que el PAN (número de cuenta principal) quede ilegible usando uno de los siguientes métodos: · Valores hash de una vía en criptografía sólida · Truncamiento · Token y ensambladores de índices (los ensambladores se deben almacenar de manera segura). · Criptografía sólida con procesos y procedimientos de administración de claves asociados. **3.4.b** Evalúe varias tablas o archivos de la muestra de repositorios de datos para controlar que el PAN (número de cuenta principal) sea ilegible (es decir, no esté almacenado en formato de texto claro). **3.4.c** Evalúe una muestra de medios extraíbles (como copias de seguridad en cintas) para confirmar que el PAN (número de cuenta principal) sea ilegible. **3.4.d** Revise una muestra de los registros de auditoría, incluidos los registros de la aplicación de pago, para confirmar que el PAN es ilegible o que no está presente en los registros. **3.4.e** Si el entorno de una entidad tiene versiones en valores hash y truncadas del mismo PAN, se deben implementar controles adicionales para asegurar que las versiones en valores hash y truncadas no se puedan correlacionar para reconstruir el PAN original.
3.4.1 Si se utiliza el cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna), se debe administrar un acceso lógico independiente y por separado de los mecanismos de autenticación y control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales ni credenciales generales de inicio de sesión de la red). Las claves de descifrado no deben estar asociadas con las cuentas de usuarios. **3.4.1.a** Si se utiliza el cifrado de disco, inspeccione la configuración y observe el proceso de autenticación a fin de verificar que el acceso lógico a los sistemas de archivos cifrados se implemente por medio de un mecanismo separado del mecanismo de autenticación del sistema operativo nativo (por ejemplo, sin utilizar bases de datos de cuentas de usuarios locales ni credenciales generales de inicio de sesión de la red). **3.4.1.b** Observe los procesos y entreviste al personal para verificar que las claves criptográficas se almacenen de forma segura (por ejemplo, se almacenan en medios extraíbles protegidos adecuadamente con controles de acceso seguros). **3.4.1.c** Revise las configuraciones y observe los procesos a fin de verificar que los datos del titular de la tarjeta almacenados en medios extraíbles se cifren en cualquier lugar donde se almacenen. **Nota:** Si no se utiliza el cifrado de disco para cifrar medios extraíbles, los datos almacenados en estos medios deberán quedar ilegibles mediante algún otro método.

Fuente: (PCI Security Standards Council, 2016)

Tabla 39 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
3.5 Documente e implemente procedimientos que protejan las claves utilizadas para proteger los datos del titular de la tarjeta almacenados contra su posible divulgación o uso indebido: 3.5 Revise las políticas y los procedimientos de administración de claves y verifique que se hayan especificado los procesos que protegen las claves utilizadas para cifrar los datos del titular de la tarjeta contra su divulgación o uso indebido y deben incluir, al menos, lo siguiente: · El acceso a las claves se restringe a la menor cantidad de custodios necesarios. · Las claves de cifrado de claves deben ser, al menos, tan sólidas como las claves de cifrado de datos que protegen. · Las claves de cifrado de claves se almacenan separadas de las claves de cifrado de datos. · Las claves se almacenan de forma segura en la menor cantidad de ubicaciones y formas posibles.
3.5.1 ***Requisitos adicionales solo para los proveedores de servicios:*** Mantenga una descripción documentada de la arquitectura criptográfica que incluye: · Detalles de todos los algoritmos, protocolos y claves utilizados para la protección de los datos del titular de la tarjeta, incluidas la complejidad de la clave y la fecha de caducidad · Descripción del uso de la clave para cada tecla · Inventario de un HSM SMS y otros SCD utilizados para la gestión de claves **3.5.1** Entreviste al personal responsable y revise la documentación para verificar que existe un documento para describir la arquitectura criptográfica, que incluye: · Detalles de todos los algoritmos, protocolos y claves utilizados para la protección de los datos del titular de la tarjeta, incluidas la complejidad de la clave y la fecha de caducidad · Descripción del uso de la clave para cada tecla · Inventario de un HSM SMS y otros SCD utilizados para la gestión de claves
3.5.2 Restrinja el acceso a las claves criptográficas a la menor cantidad de custodios necesarios. **3.5.2** Revise las listas de acceso de usuarios para controlar que el acceso a las claves se restrinja a la menor cantidad de custodios necesarios.
3.5.3 Siempre guarde las claves secretas y privadas utilizadas para cifrar/descifrar los datos del titular de la tarjeta en una (o más) de las siguientes formas: · Cifradas con una clave de cifrado de claves que sea, al menos, tan sólida como la clave de cifrado de datos y que se almacene separada de la clave de cifrado de datos. · Dentro de un dispositivo seguro criptográfico (como un HSM [módulo de seguridad de host] o un dispositivo de punto de interacción aprobado para la PTS). · Como, al menos, dos claves o componentes de la clave completos de acuerdo con los métodos aceptados por la industria. · Las claves de cifrado de claves son, al menos, tan sólidas como las claves de cifrado de datos que protegen. · Las claves de cifrado de claves se almacenan separadas de las claves de cifrado de datos.

Fuente: (PCI Security Standards Council, 2016)

Tabla 40 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
3.5.3.a Revise los procedimientos documentados para verificar que las claves criptográficas utilizadas para cifrar/descifrar los datos del titular de la tarjeta estén siempre en una (o más) de las siguientes formas en todo momento: · Cifradas con una clave de cifrado de claves que sea, al menos, tan sólida como la clave de cifrado de datos y que se almacene separada de la clave de cifrado de datos. · Dentro de un dispositivo seguro criptográfico (como un HSM [módulo de seguridad de host] o un dispositivo de punto de interacción aprobado para la PTS). · Como claves o componentes de la clave de acuerdo con los métodos aceptados por la industria. **3.5.3.b** Revise las configuraciones del sistema y las ubicaciones de almacenamiento de claves para verificar que las claves criptográficas utilizadas para cifrar/descifrar los datos del titular de la tarjeta estén siempre en una (o más) de las siguientes formas en todo momento: · Cifradas con una clave de cifrado de claves. · Dentro de un dispositivo seguro criptográfico (como un HSM [módulo de seguridad de host] o un dispositivo de punto de interacción aprobado para la PTS). · Como claves o componentes de la clave de acuerdo con los métodos aceptados por la industria. **3.5.3.c** Siempre que se usen claves de cifrado de claves, revise las configuraciones del sistema y las ubicaciones de almacenamiento de claves para verificar lo siguiente: · Las claves de cifrado de claves son, al menos, tan sólidas como las claves de cifrado de datos que protegen. · Las claves de cifrado de claves se almacenan separadas de las claves de cifrado de datos.
3.5.4 Guarde las claves criptográficas en la menor cantidad de ubicaciones posibles. **3.5.4** Revise las ubicaciones de almacenamiento de claves y observe los procesos para verificar que las claves estén almacenadas en la menor cantidad de ubicaciones posibles.
3.6 Documente por completo e implemente todos los procesos y procedimientos de administración de claves de las claves criptográficas que se utilizan para el cifrado de datos del titular de la tarjeta, incluso lo siguiente: ***Nota:*** *Varias normas de la industria relativas a la administración de claves están disponibles en distintos recursos incluido NIST, que puede encontrar en http://csrc.nist.gov.* **3.6.a *Procedimientos de pruebas adicionales solo para las evaluaciones de los proveedores de servicios:*** Si el proveedor de servicios comparte claves con sus clientes para la transmisión o el almacenamiento de datos del titular de la tarjeta, revise la documentación que el proveedor de servicios le proporciona a los clientes y verifique que incluya lineamientos sobre la manera de transmitir, almacenar y actualizar, de manera segura, sus claves, de conformidad con los Requisitos 3.6.1 a 3.6.8 que siguen a continuación. **3.6.b** Revise los procesos y procedimientos de administración de claves utilizados para cifrar los datos del titular de la tarjeta y realice lo siguiente:
3.6.1 Generación de claves de cifrado sólido **3.6.1.a** Verifique que los procedimientos de administración de claves especifiquen cómo generar claves sólidas. **3.6.1.b** Observe los procedimientos de generación de claves para verificar que se hayan generado claves sólidas.
3.6.2 Distribución segura de claves de cifrado **3.6.2.a** Verifique que los procedimientos de administración de claves especifiquen cómo distribuir las claves de manera segura. **3.6.2.b** Observe el método de distribución de claves para verificar que se distribuyan de manera segura.
3.6.3 Almacenamiento seguro de claves de cifrado **3.6.3.a** Verifique que los procedimientos de administración de claves especifiquen cómo almacenar claves de manera segura. **3.6.3.b** Observe el método de almacenamiento de claves y verifique que se almacenen de manera segura.

Fuente: (PCI Security Standards Council, 2016)

Tabla 41 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
3.6.4 La clave criptográfica cambia en el caso de las claves que han llegado al final de su período de cifrado (por ejemplo, después que haya transcurrido un período definido y/o después que cierta cantidad de texto cifrado haya sido producido por una clave dada), según lo defina el proveedor de la aplicación relacionada o el responsable de las claves, y basándose en las mejores prácticas y recomendaciones de la industria (por ejemplo, NIST Special Publication 800-57). **3.6.4.a** Verifique que los procedimientos de administración de claves incluyan un período de cifrado definido para cada tipo de clave utilizada y que definan un proceso para los cambios de clave al finalizar el período de cifrado especificado. **3.6.4.b** Entreviste al personal para verificar que se hayan cambiado las claves al finalizar el período de cifrado.
3.6.5 Retiro o reemplazo de claves (por ejemplo, mediante archivo, destrucción o revocación) según se considere necesario cuando se haya debilitado la integridad de la clave (por ejemplo, salida de la empresa de un empleado con conocimiento de una clave en texto claro, etc.) o cuando se sospeche que las claves están en riesgo. **3.6.5.a** Verifique que los procedimientos de administración de claves especifiquen procesos para realizar lo siguiente: · Retiro o reemplazo de claves cuando se haya debilitado la integridad de la clave. · Reemplazo de claves que se sepa o se sospeche que estén en riesgo. · Las claves que se conservan después de retirarlas o reemplazarlas no se usan para operaciones de cifrado. **3.6.5.b** Entreviste al personal y verifique que hayan implementado los siguientes procesos: · Las claves se retiran o reemplazan cuando se ha debilitado la integridad de la clave, incluso cuando alguien que conoce la clave deja de trabajar en la empresa. · Las claves se reemplazan si se sabe o se sospecha que están en riesgo. · Las claves que se guardan después de retirarlas o reemplazarlas no se usan para operaciones de cifrado.
3.6.6 Si se usan operaciones manuales de administración de claves criptográficas de texto claro, se deben realizar con control doble y conocimiento dividido. ***Nota:*** *Los ejemplos de operaciones manuales de administración de claves incluyen, entre otros, generación, transmisión, carga, almacenamiento y destrucción de claves.* **3.6.6.a** Verifique que los procedimientos manuales de administración de claves de texto claro especifiquen procesos para realizar lo siguiente: · Conocimiento dividido de claves, de manera tal que los componentes de las claves queden bajo control de, al menos, dos personas que solo tengan conocimiento de su propio componente de la clave. · Control doble de claves, de manera tal que se necesiten, al menos, dos personas para realizar las operaciones de administración de claves y que ninguna tenga acceso al material de autenticación del otro (por ejemplo, contraseñas o claves). **3.6.6 b** Entreviste al personal y observe los procesos para verificar que las claves manuales de texto claro se administran con lo siguiente: · Conocimiento dividido. · Control doble.
3.6.7 Prevención de sustitución no autorizada de claves criptográficas. **3.6.7.a** Verifique que los procedimientos de administración de claves especifiquen los procesos para evitar la sustitución no autorizada de claves. **3.6.7.b** Entreviste al personal y observe los procesos para verificar que se evita la sustitución no autorizada de claves.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
3.6.8 Requisito para que los custodios de claves criptográficas declaren, formalmente, que comprenden y aceptan su responsabilidad como custodios de claves. **3.6.8.a** Verifique que los procedimientos de administración de claves especifiquen los procesos para solicitar que los custodios de claves declaren (por escrito o electrónicamente) que comprenden y aceptan sus responsabilidades como custodios de claves. **3.6.8.b** Observe la documentación y otra evidencia que demuestre que los custodios de claves declararon, por escrito o electrónicamente, que comprenden y aceptan sus responsabilidades como custodios de claves.
3.7 Asegúrese de que las políticas de seguridad y los procedimientos operativos para proteger los datos del titular de la tarjeta almacenados estén documentados, implementados y que sean de conocimiento para todas las partes afectadas. **3.7** Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos para proteger los datos del titular de la tarjeta cumplan con lo siguiente: · Estén documentados, · Estén en uso, y · Sean de conocimiento para todas las partes afectadas.
4.1 Utilizar criptografía sólida y protocolos de seguridad para proteger los datos del titular de la tarjeta confidenciales durante la transmisión por redes públicas abiertas, como, por ejemplo, las siguientes: · Solo se aceptan claves y certificados de confianza. · El protocolo implementado solo admite configuraciones o versiones seguras. · La solidez del cifrado es la adecuada para la metodología de cifrado que se utiliza. **4.1.a** Identifique todas las ubicaciones donde se transmiten o reciben datos del titular de la tarjeta en redes públicas abiertas. Revise las normas documentadas y compárelas con las configuraciones del sistema para verificar que se usen protocolos de seguridad y criptografía segura en todas las ubicaciones. **4.1.b** Revise las políticas y los procedimientos documentados para verificar que se hayan especificado los procesos para las siguientes opciones: · Para aceptar solo claves o certificados de confianza. · Para que el protocolo en uso solo acepte versiones y configuraciones seguras (que no se admitan versiones ni configuraciones inseguras). · Para implementar la solidez de cifrado correcta para la metodología de cifrado que se utiliza. **4.1.c** Seleccione y observe una muestra de las transmisiones de entrada y salida a medida que ocurren (por ejemplo, observar los procesos del sistema o el tráfico de la red) para verificar que todos los datos del titular de la tarjeta se cifran con un método de criptografía sólida durante la transmisión. **4.1.d** Revise las claves y los certificados para verificar que solo se acepten claves o certificados de confianza. 4.1.c Evalúe las configuraciones del sistema y verifique que el protocolo implementado solo use configuraciones seguras y que no admita versiones ni configuraciones inseguras. **4.1.f** Evalúe las configuraciones del sistema y verifique que se implemente la solidez de cifrado correcta para la metodología de cifrado en uso. (Consulte las recomendaciones/mejores prácticas de los proveedores). **4.1.g** Para las implementaciones de TLS, revise las configuraciones del sistema y verifique que se habilite TLS al transmitir o recibir los datos del titular de la tarjeta. Por ejemplo, para implementaciones basadas en explorador: · "HTTPS" aparece como el protocolo URL (Universal Record Locator). · Los datos del titular de la tarjeta solo se solicitan si "HTTPS" aparece como parte del URL. **4.1.h** Si se utiliza SSL/TLS temprana, lleve a cabo los procedimientos de prueba

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
4.1.1 Asegúrese de que las redes inalámbricas que transmiten los datos del titular de la tarjeta o que están conectadas al entorno de datos del titular de la tarjeta utilicen las mejores prácticas de la industria a fin de implementar un cifrado sólido para la transmisión y la autenticación. **4.1.1** Identifique todas las redes inalámbricas que transmitan datos del titular de la tarjeta o que estén conectados al entorno de datos del titular de la tarjeta. Revise las normas documentadas y compárelas con los parámetros de configuración del sistema para verificar las siguientes opciones en todas las redes inalámbricas identificadas: · Se usan las mejores prácticas de la industria para implementar un cifrado sólido para la autenticación y la transmisión. · No se usa el cifrado débil (por ej., WEP, SSL) como control de seguridad para la autenticación o la transmisión.
4.2 Nunca debe enviar PAN no cifrados por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea, SMS, el chat, etc.) **4.2.a** Si se utilizan tecnologías de mensajería de usuario final para enviar los datos del titular de la tarjeta, evalúe los procesos de envío del PAN (número de cuenta principal), revise la muestra de las transmisiones salientes a medida que ocurren y verifique que el PAN (número de cuenta principal) quede ilegible o que esté protegido mediante criptografía sólida cuando se lo envía a través de tecnologías de mensajería de usuario final. **4.2.b** Revise las políticas escritas y verifique que exista una política que establezca que los PNA (número de cuenta principal) no protegidos no se deben enviar por medio de tecnologías de mensajería de usuario final
4.3 Asegúrese de que las políticas de seguridad y los procedimientos operativos para cifrar las transmisiones de los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas. **4.3** Revise la documentación, entreviste al personal y verifique que las políticas de seguridad y los procedimientos operativos para cifrar las transmisiones de los datos del titular de la tarjeta cumplen con lo siguiente: · Estén documentados, · Estén en uso, y · Sean de conocimiento para todas las partes afectadas.
5.1 Implemente un software antivirus en todos los sistemas que, generalmente, se ven afectados por software malicioso (en especial, computadoras personales y servidores). **5.1** En el caso de la muestra de componentes del sistema que incluya todos los tipos de sistemas operativos comúnmente afectados por software malicioso, verifique que se haya implementado software antivirus si existe la correspondiente tecnología antivirus.
5.1.1 Asegúrese de que los programas de antivirus puedan detectar y eliminar todos los tipos de software malicioso conocidos y proteger a los sistemas contra estos. **5.1.1** Revise la documentación del proveedor y examine las configuraciones del antivirus para verificar que los programas de antivirus realicen lo siguiente: · Detecten todos los tipos conocidos de software maliciosos. · Eliminen todos los tipos de software maliciosos conocidos. · Protejan el sistema contra todos los tipos de software maliciosos conocidos. Entre los ejemplos de tipos de software maliciosos, se pueden incluir virus, troyanos, gusanos, spyware, adware y rootkits.
5.1.2 Para aquellos sistemas que no suelen verse afectados por software maliciosos, lleve a cabo evaluaciones periódicas para identificar y evaluar las amenazas de malware que pueden aparecer a fin de determinar si es necesario o no implementar un software antivirus en dichos sistemas. **5.1.2** Entreviste al personal para verificar que se supervisan y evalúan las amenazas de malware en aquellos sistemas que no suelen verse afectados por software maliciosos a fin de determinar si es necesario o no implementar un software antivirus en dichos sistemas.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
5.2 Asegúrese de que los mecanismos de antivirus cumplan con lo siguiente: · Estén actualizados. · Ejecuten análisis periódicos. · Generen registros de auditoría que se guarden de conformidad con el Requisito 10.7 de las PCI DSS. **5.2.a** Revise las políticas y los procedimientos para verificar que las definiciones y el software antivirus exijan actualizaciones. **5.2.b** Revise las configuraciones de antivirus, incluso la instalación maestra del software, para verificar lo siguiente en los mecanismos de antivirus: · Estén configurados para realizar actualizaciones automáticas. · Estén configurados para realizar análisis periódicos. **5.2.c** Revise una muestra de los componentes del sistema, incluso todos los tipos de sistemas operativos comúnmente afectados por software malicioso, a fin de controlar lo siguiente: · Las definiciones y el software antivirus estén actualizados. · Se realicen análisis periódicos. **5.2.d** Revise las configuraciones de antivirus, incluso la instalación maestra del software y una muestra de los componentes del sistema, para verificar lo siguiente: · La generación de registro de software antivirus esté habilitada. · Los registros se conserven de acuerdo con el Requisito 10.7 de las PCI DSS.
5.3 Asegúrese de que los mecanismos de antivirus funcionen activamente y que los usuarios no puedan deshabilitarlos ni alterarlos, salvo que estén específicamente autorizados por la gerencia en casos particulares y durante un período limitado. Nota: Las soluciones de antivirus se pueden desactivar temporalmente, pero solo si existe una necesidad técnica legítima como en el caso de la autorización de la gerencia en casos particulares. Si es necesario desactivar la protección de antivirus por un motivo específico, se debe contar con una autorización formal. Es posible que sea necesario implementar medidas de seguridad adicionales en el período en que no esté activa la protección de antivirus. **5.3.a** Revise las configuraciones de antivirus, incluso la instalación maestra del software y una muestra de los componentes del sistema, para verificar que el software antivirus funcione activamente. **5.3.b** Revise las configuraciones de antivirus, incluso la instalación maestra del software y una muestra de los componentes del sistema, para verificar que los usuarios no puedan deshabilitar ni modificar el software antivirus. **5.3.c** Entreviste al personal responsable y evalúe los procesos para verificar que los usuarios no puedan deshabilitar ni modificar el software antivirus, salvo que estén específicamente autorizados por la gerencia en casos particulares y durante un período limitado.
5.4 Asegúrese de que las políticas de seguridad y los procedimientos operativos que protegen los sistemas estén documentados, implementados y que sean de conocimiento para todas las partes afectadas. **5.4** Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos que protegen el sistema contra malware cumplen con lo siguiente: · Estén documentados, · Estén en uso, y · Sean de conocimiento para todas las partes afectadas.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
6.1 Establezca un proceso para identificar las vulnerabilidades de seguridad por medio de fuentes externas conocidas para obtener información sobre las vulnerabilidades de seguridad, y asigne una clasificación de riesgo (por ejemplo, “alto”, “medio” o “bajo”) a las vulnerabilidades de seguridad recientemente descubiertas. Nota: Las clasificaciones de riesgo se deben basar en las mejores prácticas de la industria y en el posible impacto. Por ejemplo, en los criterios para clasificar las vulnerabilidades, se puede tener en cuenta la puntuación base CVSS, la clasificación del proveedor o el tipo de sistema afectado. Los métodos para evaluar las vulnerabilidades y asignar las clasificaciones de riesgo varían según el entorno y la estrategia de evaluación de riesgos de la organización. Las clasificaciones de riesgo deben identificar, mínimamente, todas las vulnerabilidades que se consideren de “alto riesgo” para el entorno. Además de la clasificación de riesgos, las vulnerabilidades se pueden considerar “críticas” si suponen una amenaza inminente para el entorno, si afectan los sistemas o si generan un posible riesgo si no se contemplan. Algunos ejemplos de sistemas críticos son los sistemas de seguridad, los dispositivos y sistemas públicos, las bases de datos y otros sistemas que almacenan, procesan o transmiten datos del titular de la tarjeta. **6.1.a** Revise las políticas y los procedimientos y verifique que los procesos estén definidos para realizar lo siguiente: · Identificar nuevas vulnerabilidades de seguridad. · Asignar una clasificación de riesgo a las vulnerabilidades en la que se identifiquen todas las vulnerabilidades de “alto riesgo” y “críticas”. · Usar fuentes externas conocidas para obtener información sobre las vulnerabilidades de seguridad. **6.1.b** Entreviste al personal y observe el proceso para verificar lo siguiente: · Se identifiquen nuevas vulnerabilidades de seguridad. · Se asigne una clasificación de riesgo a las vulnerabilidades que identifique todas las vulnerabilidades de “alto riesgo” y “críticas”. · Los procesos que identifican las nuevas vulnerabilidades de seguridad incluyen usar fuentes externas conocidas para obtener información sobre vulnerabilidades de seguridad.
6.2 Asegúrese de que todos los software y componentes del sistema tengan instalados parches de seguridad proporcionados por los proveedores que ofrecen protección contra vulnerabilidades conocidas. Instale los parches importantes de seguridad dentro de un plazo de un mes de su lanzamiento. Nota: Los parches de seguridad críticos se deben identificar de conformidad con el proceso de clasificación de riesgos definido en el Requisito 6.1. **6.2.a** Revise las políticas y los procedimientos de instalación de parches de seguridad a fin de verificar que los procesos estén definidos para realizar lo siguiente: · Instalación de parches de seguridad críticos proporcionados por el proveedor dentro del mes del lanzamiento. · Instalación de todos los parches de seguridad proporcionados por el proveedor en un período coherente (por ejemplo, en un período de tres meses). **6.2.b** En el caso de una muestra de los componentes del sistema y del software relacionado, compare la lista de parches de seguridad instalados en cada sistema con la última lista de parches de seguridad proporcionados por el proveedor para verificar lo siguiente: · Los parches de seguridad críticos correspondientes proporcionados por el proveedor se instalen dentro del mes del lanzamiento. · Todos los parches de seguridad correspondientes proporcionados por el proveedor se instalen en un período específico (por ejemplo, en un plazo de tres meses).

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
6.3 Desarrolle aplicaciones de software internas y externas (incluso acceso administrativo a aplicaciones basado en web) de manera segura y de la siguiente manera: · De acuerdo con las PCI DSS (por ejemplo, autenticación y registros seguros). · Basadas en las normas o en las mejores prácticas de la industria. · Incorporación de seguridad de la información durante todo el ciclo de vida del desarrollo del software. **Nota:** Esto rige para todos los softwares desarrollados internamente y para todos los softwares personalizados desarrollados externamente. **6.3.a** Revise los procesos de desarrollo de software escritos para verificar que se basen en las normas o en las mejores prácticas de la industria. **6.3.b** Revise los procesos de desarrollo de software escritos y verifique que se incluya la seguridad de la información durante todo el ciclo de vida. **6.3.c** Evalúe los procesos de desarrollo de software escritos y verifique que las aplicaciones de software se desarrollen de conformidad con las PCI DSS. **6.3.d** Entreviste a los desarrolladores de software para verificar que se implementen los procesos de desarrollo de software escritos.
6.3.1 Elimine las cuentas de desarrollo, de prueba y de aplicaciones personalizadas, las ID de usuario y las contraseñas antes de que las aplicaciones se activen o se pongan a disposición de los clientes. **6.3.1** Revise los procedimientos de desarrollo de software escritos y entreviste al personal responsable a fin de verificar que la producción previa y las cuentas de aplicaciones personalizadas, las ID de usuarios y las contraseñas se eliminen antes de enviar la aplicación a producción o ponerla a disposición de los clientes.
6.3.2 Revise el código personalizado antes de enviarlo a producción o de ponerlo a disposición de los clientes a fin de identificar posibles vulnerabilidades en la codificación (mediante procesos manuales o automáticos) y que incluya, al menos, lo siguiente: · La revisión de los cambios en los códigos está a cargo de personas que no hayan creado el código y que tengan conocimiento de técnicas de revisión de código y prácticas de codificación segura. · Las revisiones de los códigos deben garantizar que el código se desarrolle de acuerdo con las directrices de codificación segura. · Las correcciones pertinentes se implementan antes del lanzamiento. · La gerencia revisa y aprueba los resultados de la revisión de códigos antes del lanzamiento. **6.3.2.a** Revise los procedimientos de desarrollo de software escritos y entreviste al personal responsable para verificar que todos los cambios de código de las aplicaciones personalizadas (ya sea mediante procesos manuales o automáticos) se revisen de la siguiente manera: · Individuos que no sean el autor que originó el código e individuos con conocimiento en técnicas de revisión de código y prácticas de codificación segura revisan los cambios en los códigos. · Las revisiones de los códigos aseguran que estos se desarrollan de acuerdo con las directrices de codificación segura (consulte el requisito 6.5 de las PCI DSS). · Las correcciones pertinentes se implementan antes del lanzamiento. · La gerencia revisa y aprueba los resultados de la revisión de códigos antes del lanzamiento. **6.3.2.b** Seleccione una muestra de los cambios recientes de las aplicaciones personalizadas y verifique que los códigos de aplicaciones personalizadas se revisen de acuerdo con el punto 6.3.2.a mencionado anteriormente.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
6.4 Siga los procesos y procedimientos de control de todos los cambios en los componentes del sistema. Los procesos deben incluir lo siguiente: **6.4** Revise las políticas y los procedimientos y verifique que se define lo siguiente: · Los entornos de prueba/desarrollo están separados del entorno de producción y se implementa un control de acceso para reforzar la separación. · Existe una separación de funciones entre el personal asignado a los entornos de desarrollo/prueba y el personal asignado al entorno de producción. · Los datos de producción (PAN activos) no se usan en las pruebas ni en el desarrollo. · Los datos y las cuentas de prueba se eliminan antes de que se active el sistema de producción. · Se documentan los procedimientos de control de cambios relacionados con la implementación de parches de seguridad y las modificaciones del software.
6.4.1 Separe los entornos de desarrollo/prueba de los entornos de producción y refuerce la separación con controles de acceso. **6.4.1.a** Revise la documentación de la red y la configuración de los dispositivos de red a fin de verificar que los entornos de desarrollo/prueba estén separados de los entornos de producción. **6.4.1.b** Revise la configuración de los controles de acceso y verifique que se implementen estos controles para reforzar la separación entre los entornos de desarrollo/prueba y los entornos de producción.
6.4.2 Separación de funciones entre desarrollo/prueba y entornos de producción **6.4.2** Observe los procesos y entreviste al personal asignado a los entornos de desarrollo/prueba y al personal asignado al entorno de producción para verificar que se implementen las tareas de separación entre los entornos de desarrollo/prueba y el de producción.
6.4.3 Los datos de producción (PAN activos) no se utilizan para las pruebas ni para el desarrollo **6.4.3.a** Observe los procesos de pruebas y entreviste al personal para verificar que se implementen los procedimientos a fin de garantizar que los datos de producción (PAN activos) no se usen en las pruebas ni en el desarrollo. **6.4.3.b** Revise una muestra de datos de pruebas para verificar que los datos de producción (PAN activos) no se utilicen en las pruebas ni en el desarrollo.
6.4.4 Eliminación de datos y cuentas de los componentes del sistema antes de que se activen los sistemas de producción **6.4.4.a** Observe los procesos de pruebas y entreviste al personal para verificar que las cuentas y los datos de pruebas se eliminen antes de activar el sistema de producción. **6.4.4.b** Revise una muestra de los datos y las cuentas del sistema de producción recientemente instalado o actualizado para verificar que los datos y las cuentas se eliminen antes de activar el sistema.
6.4.5 Los procedimientos de control de cambios deben incluir lo siguiente: **6.4.5.a** Revise los procedimientos de control de cambios documentados y verifique que los procedimientos estén definidos según lo siguiente: · Documentación de incidencia · Aprobación de cambio documentada por las partes autorizadas. · Pruebas de funcionalidad a fin de verificar que el cambio no impacta negativamente en la seguridad del sistema. · Procedimientos de desinstalación **6.4.5.b** En el caso de una muestra de componentes del sistema, entreviste al personal responsable para determinar los cambios recientes. Realice un seguimiento de los cambios relacionados con la documentación del control de cambios. Por cada cambio que evalúe, realice lo siguiente:

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
6.4.5.1 Documentación de incidencia. **6.4.5.1** Verifique que la documentación de incidencia se incluya en la documentación del control de cambios de cada muestra de cambio. **6.4.5.2** Aprobación de cambio documentada por las partes autorizadas. **6.4.5.2** Verifique que la aprobación documentada por las partes autorizadas esté presente para cada muestra de cambio. **6.4.5.3** Verifique que se hayan realizado las pruebas de funcionalidad y que el cambio no impacte negativamente en la seguridad del sistema. **6.4.5.3.a** En el caso de las muestras de cambio, revise que las pruebas de funcionalidad se hayan realizado para verificar que el cambio no impacte negativamente en la seguridad del sistema. **6.4.5.3.b** En el caso de los cambios del código personalizado, verifique que se hayan realizado las pruebas a todas las actualizaciones de conformidad con el Requisito 6.5 de las PCI DSS antes de la implementación en producción. **6.4.5.4** Procedimientos de desinstalación. **6.4.5.4** Verifique que se preparen los procedimientos de desinstalación para cada muestra de cambio.
6.4.6 Al término de un cambio significativo, deben implementarse todos los requisitos pertinentes de la PCI DSS en todos los sistemas y redes nuevos o modificados, y la documentación actualizada según sea el caso. **Nota:** Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito. **6.4.6** Para una muestra de los cambios significativos, revise los registros de cambios, entreviste al personal, y observe los sistemas/redes afectados para verificar que se implementaron los requisitos aplicables de la PCI DSS y que se actualizó la documentación como parte del cambio.
6.5.1 Errores de inyección, en especial, errores de inyección SQL. También considere los errores de inyección de comandos de OS, LDAP y Xpath, así como otros errores de inyección. **6.5.1** Evalúe las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que las técnicas de codificación aborden los errores de inyección y realicen lo siguiente: · Validación de la entrada para comprobar que los datos de los usuarios no puedan modificar el significado de los comandos ni de las consultas. · Uso de consultas basadas en parámetros.
6.5.2 Desbordamiento de buffer **6.5.2** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que las técnicas de codificación aborden los desbordamientos de buffer y realicen lo siguiente: · Validación de los límites del buffer. · Truncamiento de cadenas de entrada.
6.5.3 Almacenamiento cifrado inseguro **6.5.3** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que las técnicas de codificación aborden el almacenamiento criptográfico inseguro y realicen lo siguiente: · Prevenga errores de cifrado. · Utilice claves y algoritmos criptográficos sólidos.
6.5.4 Comunicaciones inseguras **6.5.4** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que se aborden las comunicaciones inseguras mediante técnicas de codificación que autentique y cifren correctamente todas las comunicaciones confidenciales:

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
6.5.5 Manejo inadecuado de errores **6.5.5** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que el manejo inadecuado de errores se corrige mediante técnicas de codificación que no filtran información por medio de mensajes de error (por ejemplo, enviando detalles genéricos del error, en lugar de enviar detalles específicos).
6.5.6 Todas las vulnerabilidades de "alto riesgo" detectadas en el proceso de identificación de vulnerabilidades (según lo definido en el Requisito 6.1 de las PCI DSS). **6.5.6** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable para verificar que las técnicas de codificación aborden las vulnerabilidades de "alto riesgo" que puedan afectar la aplicación, según lo especificado en el Requisito 6.1 de las PCI DSS. ***Nota**: Los Requisitos 6.5.7 al 6.5.10, que siguen a continuación, rigen para las aplicaciones web y las interfaces de las aplicaciones (internas o externas):*
6.5.7 Lenguaje de comandos entre distintos sitios (XSS) **6.5.7** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que el XSS (lenguaje de comandos entre distintos sitios) se aborde con las técnicas de codificación que incluyen lo siguiente: · Validación de todos los parámetros antes de la inclusión. · Uso de técnicas de escape sensibles al contexto.
6.5.8 Control de acceso inapropiado (como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios, y la no restricción de acceso a las funciones por parte de los usuarios). **6.5.8** Evalúe las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable para verificar que el control de acceso inapropiado, como las referencias no seguras a objetos directos, la no restricción de acceso a URL y la exposición completa de los directorios, se aborde mediante técnicas de codificación que incluyan lo siguiente: · Autenticación correcta de usuarios. · Desinfección de entradas. · No exposición de referencias a objetos internos a usuarios. Interfaces de usuarios que no permitan el acceso a funciones no autorizadas.
6.5.9 Falsificación de solicitudes entre distintos sitios (CSRF) **6.5.9** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable para verificar que, para corregir la CSRF (falsificación de solicitudes entre distintos sitios), se utilicen técnicas de codificación que aseguren que las aplicaciones no confían en las credenciales de autorización ni en los tokens que los exploradores presentan automáticamente.
6.5.10 Autenticación y administración de sesión interrumpidas **6.5.10** Revise las políticas y los procedimientos de desarrollo de software y entreviste al personal responsable a fin de verificar que la autenticación y la administración de sesión interrumpidas se aborden con técnicas de codificación que, generalmente, incluyen lo siguiente: · Marcas de tokens de sesión (por ejemplo, cookies) como "seguros". · No exposición de las ID de la sesión en el URL. · Incorporación de tiempos de espera apropiados y rotación de las ID de la sesión después de iniciar sesión satisfactoriamente.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
6.6 En el caso de aplicaciones web públicas, trate las nuevas amenazas y vulnerabilidades continuamente y asegúrese de que estas aplicaciones se protejan contra ataques conocidos con alguno de los siguientes métodos: · Controlar las aplicaciones web públicas mediante herramientas o métodos de evaluación de seguridad de vulnerabilidad de aplicación automáticas o manuales, por lo menos, anualmente y después de cada cambio · Revise los parámetros de la configuración del sistema y entreviste al personal responsable para verificar que se haya implementado una solución técnica automática que detecte y prevenga ataques web (por ejemplo, un firewall de aplicación web) de la siguiente manera: - Se encuentre delante de las aplicaciones web públicas para detectar y prevenir ataques web. - Funcione activamente y esté actualizada, según corresponda. - Genere registros de auditoría. - Esté configurada para bloquear ataques web o para generar una alerta que se investiga de inmediato.
6.7 Asegúrese de que las políticas de seguridad y los procedimientos operativos para desarrollar y mantener seguros los sistemas y las aplicaciones estén documentados, implementados y que sean de conocimiento para todas las partes afectadas. **6.7** Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos para desarrollar y mantener seguros los sistemas y las aplicaciones cumplen con lo siguiente: · Estén documentados, · Estén en uso, y · Sean de conocimiento para todas las partes afectadas.
7.1 Limite el acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso. **7.1** Revise las políticas escritas para el control de acceso y verifique que incorporen los Requisitos 7.1.1 al 7.1.4 de la siguiente manera: · Definición de las necesidades de acceso y asignación de privilegios de cada función. · Restricción de acceso de usuarios con ID privilegiadas a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo. · Asignación de acceso según la tarea, la clasificación y la función de cada persona. · Aprobación documentada (por escrito o electrónicamente) de las partes autorizadas para todos los accesos, que incluye la lista de los privilegios específicos aprobados.
7.1.1 Defina las necesidades de acceso de cada función, incluso lo siguiente: · Los componentes del sistema y los recursos de datos que necesita cada función para acceder a fin de realizar su trabajo. · Nivel de privilegio necesario (por ejemplo, usuario, administrador, etc.) para acceder a los recursos. **7.1.1** Seleccione una muestra de funciones y verifique que las necesidades de acceso de cada función estén definidas e incluyan lo siguiente: · Los componentes del sistema y los recursos de datos que necesita cada función para acceder a fin de realizar su trabajo. · Identificación de los privilegios necesarios de cada función para que puedan desempeñar sus funciones.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
7.1.2 Limite el acceso de usuarios con ID privilegiadas a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo. **7.1.2.a** Entreviste al personal responsable de asignar los accesos para verificar que el acceso de usuarios con ID privilegiadas cumple con lo siguiente: · Se asigna solamente a las funciones que específicamente necesitan acceso privilegiado. · Estén restringidos a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo. **7.1.2.b** Seleccione una muestra de las ID de usuarios con acceso privilegiado y entreviste al personal de administración responsable a fin de verificar que los privilegios asignados respeten lo siguiente: · Sean necesarios para el trabajo de la persona. · Estén restringidos a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo.
7.1.3 Asigne el acceso según la tarea, la clasificación y la función del personal. **7.1.3** Seleccione una muestra de las ID de usuarios y entreviste al personal de administración responsable para verificar que los privilegios se asignen según la clasificación y la función laboral de la persona.
7.1.4 Solicite la aprobación documentada de las partes autorizadas en la que se especifiquen los privilegios necesarios. **7.1.4** Seleccione una muestra de las ID de usuario y compárelas con la aprobación documentada para verificar lo siguiente: · Exista una aprobación documentada para los privilegios asignados. · Las partes autorizadas realizaron la aprobación. · Los privilegios especificados coinciden con los roles asignados a la persona.
7.2 Establezca un sistema de control de acceso para los componentes del sistema que restrinja el acceso según la necesidad del usuario de conocer y que se configure para “negar todo”, salvo que se permita específicamente. Este sistema de control de acceso debe incluir lo siguiente: **7.2** Evalúe los parámetros del sistema y la documentación del proveedor para verificar que el sistema de control de acceso se implemente de la siguiente manera:
7.2.1 Cobertura de todos los componentes del sistema **7.2.1** Confirme que los sistemas de control de acceso se implementen en todos los componentes del sistema.
7.2.2 La asignación de privilegios a una persona se basa en la clasificación del trabajo y su función. **7.2.2** Confirme que los sistemas de control de acceso estén configurados de manera tal que los privilegios asignados a una persona se realicen según la clasificación del trabajo y la función.
7.2.3 Configuración predeterminada de “negar todos”. **7.2.3** Confirme que los sistemas de control de acceso cuenten con la configuración predeterminada de “negar todos”.
7.3 Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas. **7.3** Revise la documentación, entreviste al personal y verifique que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta cumplan con lo siguiente: · Estén documentados, · Estén en uso, y · Sean de conocimiento para todas las partes afectadas.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
8.1 Defina e implemente políticas y procedimientos para garantizar la correcta administración de la identificación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema de la siguiente manera: **8.1.a** Revise los procedimientos y confirme que definen procesos para cada uno de los siguientes puntos, desde el 8.1.1 hasta el 8.1.8. **8.1.b** Verifique que se implementen los procedimientos para la administración de identificación de usuarios mediante las siguientes acciones:
8.1.1 Asigne a todos los usuarios una ID exclusiva antes de permitirles acceder a los componentes del sistema o a los datos del titular de la tarjeta. **8.1.1** Entreviste al personal administrativo y confirme que todos los usuarios tengan asignada una ID exclusiva para tener acceso a los componentes del sistema o los datos del titular de la tarjeta.
8.1.2 Controle la incorporación, la eliminación y la modificación de las ID de usuario, las credenciales y otros objetos de identificación. **8.1.2** En el caso de una muestra de ID de usuarios privilegiados e ID de usuarios generales, evalúe las autorizaciones asociadas y observe los parámetros del sistema a fin de verificar que todas las ID de usuarios y las ID de usuarios privilegiados se hayan implementado solamente con los privilegios especificados en la aprobación documentada.
8.1.3 Cancele de inmediato el acceso a cualquier usuario cesante. **8.1.3.a** Seleccione una muestra de los usuarios cesantes en los últimos seis meses y revise las listas de acceso de usuarios actuales, tanto para acceso local como remoto, para verificar que sus ID se hayan desactivado o eliminado de las listas de acceso. **8.1.3.b** Verifique que todos los métodos de autenticación físicos, como tarjetas inteligentes, tokens, etc., se hayan devuelto o desactivado.
8.1.4 Elimine o inhabilite las cuentas de usuario inactivas, al menos, cada 90 días. **8.1.4** Observe las cuentas de usuarios y verifique que se eliminen o inhabiliten las que lleven más de 90 días inactivas.
8.1.5 Administre las ID que usan los terceros para acceder, respaldar o mantener los componentes del sistema de manera remota de la siguiente manera: · Se deben habilitar solamente durante el tiempo que se necesitan e inhabilitar cuando no se usan. · Se deben monitorear mientras se usan. **8.1.5.a** Entreviste al personal y observe los procesos de administración de cuentas que usan los proveedores para acceder, respaldar o mantener los componentes del sistema a fin de verificar que las cuentas que usan los proveedores para acceder de manera remota cumplen con lo siguiente: · Se inhabilitan cuando no se usan. · Se habilitan solo cuando el proveedor las necesita y se deshabilitan cuando no se usan. **8.1.5.b** Entreviste al personal y observe los procesos para verificar que se monitoreen las cuentas de acceso remoto de los terceros mientras se utilizan.
8.1.6 Limite los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos. **8.1.6.a** En el caso de una muestra de componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de autenticación se encuentren configurados de manera que se solicite que se bloquee la cuenta del usuario después de realizar, como máximo, seis intentos de inicio de sesión no válidos. **8.1.6.b** Procedimientos de pruebas adicionales para los proveedores de servicios: Revise los procesos internos y la documentación del cliente/usuario y observe los procesos implementados a fin de verificar que las cuentas de usuarios no consumidores se bloqueen de forma temporal después de realizar, como máximo, seis intentos no válidos de acceso.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
8.1.7 Establezca la duración del bloqueo a un mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario. **8.1.7** En el caso de una muestra de componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas se encuentren configurados de manera que solicite que, al bloquear la cuenta de un usuario, esta permanezca bloqueada un mínimo de 30 minutos o hasta que el administrador del sistema la restablezca.
8.1.8 Si alguna sesión estuvo inactiva durante más de 15 minutos, solicite al usuario que vuelva a escribir la contraseña para activar la terminal o la sesión nuevamente. **8.1.8** En el caso de una muestra de componentes del sistema, inspeccione los parámetros de
8.2 Además de asignar una ID exclusiva, asegúrese de que haya una correcta administración de autenticación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema y que se use, al menos, uno de los siguientes métodos para autenticar
8.2.1 Deje ilegibles todas las credenciales de autenticación (como contraseñas/frases) durante la transmisión y el almacenamiento en todos los componentes del sistema mediante una criptografía sólida. **8.2.1.a** Evalúe la documentación del proveedor y los parámetros de configuración del sistema para verificar que las contraseñas se protegen durante la transmisión y el almacenamiento mediante una criptografía sólida. **8.2.1.b** En el caso de una muestra de componentes del sistema, revise los archivos de las contraseñas para verificar que sean ilegibles durante el almacenamiento. **8.2.1.c** En el caso de una muestra de los componentes del sistema, revise la transmisión de datos para verificar que las contraseñas sean ilegibles durante la transmisión. **8.2.1.d** Procedimientos de pruebas adicionales para los proveedores de servicios: Observe los archivos de contraseñas y verifique que las contraseñas de los clientes sean ilegibles durante el almacenamiento. **8.2.1.e** Procedimientos de pruebas adicionales solo para los proveedores de servicios: Observe los archivos de contraseñas y verifique que las contraseñas de los clientes sean ilegibles durante la transmisión.
8.2.2 Verifique la identidad del usuario antes de modificar alguna credencial de autenticación, por ejemplo, restablezca la contraseña, entregue nuevos tokens o genere nuevas claves. **8.2.2** Revise los procedimientos de autenticación para modificar las credenciales de autenticación

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
8.2.3 Las contraseñas/frases deben tener lo siguiente: · Una longitud mínima de siete caracteres. · Combinación de caracteres numéricos y alfabéticos. De manera alternativa, la contraseña/frase debe tener una complejidad y una solidez, al menos, equivalente a los parámetros que se especifican anteriormente. **8.2.3a** En el caso de una muestra de los componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de la contraseña del usuario se encuentren configurados de manera que soliciten, al menos, la siguiente solidez o complejidad: · Una longitud mínima de siete caracteres. · Combinación de caracteres numéricos y alfabéticos. **8.2.3.b** Procedimientos de pruebas adicionales para los proveedores de servicios: Revise los procesos internos y la documentación del cliente/usuario para verificar que se solicite que las contraseñas de usuarios no consumidores cumplan, al menos, con la siguiente solidez o complejidad: · Una longitud mínima de siete caracteres. · Combinación de caracteres numéricos y alfabéticos.
8.2.4 Cambie la contraseña/frase de usuario, al menos, cada 90 días. **8.2.4.a** En el caso de una muestra de componentes del sistema, inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas de usuario se encuentren configurados de manera que se le solicite al usuario cambiar su contraseña, al menos, cada 90 días. **8.2.4.b** Procedimientos de pruebas adicionales solo para los proveedores de servicios: Revise los procesos internos y la documentación del cliente/usuario y verifique lo siguiente: · Las contraseñas de usuarios no consumidores se deben cambiar periódicamente; y · Se debe orientar a los usuarios no consumidores sobre cuándo y en qué situaciones deben cambiar las contraseñas.
8.2.5 No permita que una persona envíe una contraseña/frase nueva que sea igual a cualquiera de las últimas cuatro contraseñas/frases utilizadas. **8.2.5.a** Para una muestra de componentes del sistema, obtenga e inspeccione los parámetros de configuración del sistema para verificar que los parámetros de las contraseñas se encuentren configurados para que soliciten que las nuevas contraseñas no sean iguales a las últimas cuatro contraseñas utilizadas. **8.2.5.b** Procedimientos de pruebas adicionales para los proveedores de servicios: Revise los procesos internos y la documentación del cliente/usuario para verificar que las nuevas contraseñas de usuarios no consumidores no puedan ser iguales a las últimas cuatro contraseñas utilizadas anteriormente.
8.2.6 Configure la primera contraseña/frase y las restablecidas en un valor único para cada usuario y cámbiela de inmediato después del primer uso. **8.2.6** Revise los procedimientos de contraseña y observe al personal de seguridad para verificar que las primeras contraseñas para nuevos usuarios, y las contraseñas restablecidas para usuarios existentes, se configuren en un valor único para cada usuario y se cambien después del primer uso.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
8.3 Asegure todo el acceso administrativo individual que no sea de consola y todo el acceso remoto al CDE mediante la autenticación de múltiples factores. Nota: La autenticación de múltiples factores requiere que se utilicen dos de los tres métodos de autenticación (consulte el Requisito 8.2 para obtener una descripción de los métodos de autenticación). El uso de un mismo factor dos veces (por ejemplo, utilizar dos contraseñas individuales) no se considera una autenticación de múltiples factores.
8.3.1 Incorporar la autenticación de múltiples factores para todo acceso que no sea de consola en el CDE para el personal con acceso administrativo. **8.3.1.a** Revise las configuraciones de la red y/o sistema, según sea el caso, para verificar que la autenticación de múltiples factores se requiere para todo el acceso administrativo que no es de consola en el CDE. **8.3.1.b** Observe un grupo de empleados (por ejemplo, usuarios y administradores) que se conectan de manera remota al CDE y verifique que se usen, al menos, dos de los tres métodos de autenticación.
8.3.2 Incorpore la autenticación de múltiples factores para todo acceso remoto que se origine desde fuera de la red de la entidad (tanto para usuarios como administradores, e incluso para todos los terceros involucrados en el soporte o mantenimiento). **8.3.2.a** Revise la configuración del sistema para los servidores y sistemas de acceso remoto, y verifique que se exija la autenticación de múltiples factores en los siguientes casos: · Todo el acceso remoto por parte del personal, tanto del usuario como del administrador, y · Acceso remoto de todos los terceros/proveedores (incluye el acceso a aplicaciones y componentes del sistema para soporte o mantenimiento). **8.3.2.b** Observe una muestra de empleados (por ejemplo, usuarios y administradores) que se conectan de manera remota a la red y verifique que se usen, al menos, dos de los tres métodos de autenticación.
8.4 Documente y comunique los procedimientos y las políticas de autenticación a todos los usuarios, que incluye lo siguiente: · Lineamientos sobre cómo seleccionar credenciales de autenticación sólidas. · Lineamientos sobre cómo los usuarios deben proteger las credenciales de autenticación. · Instrucciones para no seleccionar contraseñas utilizadas anteriormente. · Instrucciones para cambiar contraseñas si se sospecha que la contraseña corre riesgos. **8.4.a** Revise los procedimientos y entreviste al personal para verificar que los procedimientos y las políticas de autenticación se distribuyen a todos los usuarios. **8.4.b** Revise los procedimientos y las políticas de autenticación que se le entregan a los usuarios y verifique que incluyan lo siguiente: · Lineamientos sobre cómo seleccionar credenciales de autenticación sólidas. · Lineamientos sobre cómo los usuarios deben proteger las credenciales de autenticación. · Instrucciones para los usuarios para que no seleccionen contraseñas utilizadas anteriormente. · Instrucciones para cambiar contraseñas si se sospecha que la contraseña corre riesgos. **8.4.c** Entreviste a un grupo de usuarios y verifique que conozcan los procedimientos y las políticas de autenticación.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
8.5 No use ID ni contraseñas de grupo, compartidas ni genéricas, ni otros métodos de autenticación de la siguiente manera: · Las ID de usuario genéricas se deben desactivar o eliminar. · No existen ID de usuario compartidas para realizar actividades de administración del sistema y demás funciones críticas. · Las ID de usuario compartidas y genéricas no se utilizan para administrar componentes del sistema. **8.5.a** En el caso de una muestra de los componentes del sistema, revise las listas de ID de usuarios y verifique lo siguiente: · Las ID de usuario genéricas se deben desactivar o eliminar. · No existen ID de usuario compartidas para realizar actividades de administración del sistema y demás funciones críticas. · Las ID de usuario compartidas y genéricas no se utilizan para administrar componentes del sistema. **8.5.b** Revise las políticas y los procedimientos de autenticación y verifique que el uso de ID y/o contraseñas u otros métodos de autenticación grupales y compartidos estén explícitamente prohibidos. **8.5.c** Entreviste a los administradores del sistema y verifique que las contraseñas de grupo y compartidas u otros métodos de autenticación no se distribuyan, incluso si se solicitan.
8.5.1 Requisitos adicionales solo para los proveedores de servicios: Los proveedores de servicios que tengan acceso a las instalaciones del cliente (por ejemplo, para tareas de soporte de los sistemas de POS o de los servidores) deben usar una credencial de autenticación exclusiva (como una contraseña/frase) para cada cliente. **8.5.1** Procedimientos de pruebas adicionales solo para los proveedores de servicios: Revise las políticas y los procedimientos de autenticación y entreviste al personal para verificar que se utilicen diferentes credenciales de autenticación para acceder a cada cliente.
8.6 Si se utilizan otros mecanismos de autenticación (por ejemplo, tokens de seguridad físicos o lógicos, tarjetas inteligentes, certificados, etc.), el uso de estos mecanismos se debe asignar de la siguiente manera: · Los mecanismos de autenticación se deben asignar a una sola cuenta y no compartirlos entre varias. · Se deben implementar controles físicos y lógicos para garantizar que solo la cuenta deseada usa esos mecanismos para acceder. **8.6.a** Revise las políticas y los procedimientos de autenticación para verificar que los procedimientos que usan mecanismos de autenticación, como tokens de seguridad físicos, tarjetas inteligentes y certificados, estén definidos e incluyan lo siguiente: · Los mecanismos de autenticación se asignan a una sola cuenta y no se comparten entre varias. · Los controles físicos y lógicos se definen para garantizar que solo la cuenta deseada usa esos mecanismos para acceder. **8.6.b** Entreviste al personal de seguridad y verifique que se asignen mecanismos de autenticación a una sola cuenta y que no se compartan entre varias. **8.6.c** Examine los parámetros de configuración del sistema y los controles físicos, según corresponda, para verificar que se implementen controles a fin de garantizar que solo la cuenta deseada usa esos mecanismos para acceder.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
8.7 Se restringen todos los accesos a cualquier base de datos que contenga datos del titular de la tarjeta (que incluye acceso por parte de aplicaciones, administradores y todos los otros usuarios) de la siguiente manera: · Todo acceso, consultas y acciones de usuario en las bases de datos se realizan, únicamente, mediante métodos programáticos. · Solo los administradores de la base de datos pueden acceder directamente a las bases de datos o realizar consultas en estas. · Solo las aplicaciones pueden usar las ID de aplicaciones para las aplicaciones de base de datos (no las pueden usar los usuarios ni otros procesos que no pertenezcan a la aplicación). **8.7.a** Revise los parámetros de configuración de la aplicación y de la base de datos, y verifique que todos los usuarios estén autenticados antes de acceder. **8.7.b** Revise los parámetros de configuración de la base de datos y de la aplicación para verificar que el acceso de todos los usuarios, las consultas del usuario y las acciones del usuario (por ejemplo, mover, copiar, eliminar) en la base de datos se realicen únicamente mediante métodos programáticos (por ejemplo, a través de procedimientos almacenados). **8.7.c** Evalúe los parámetros de control de acceso de la base de datos y los parámetros de configuración de la aplicación de la base de datos y verifique que el acceso directo del usuario a la base de datos, o las consultas a esta, esté limitado a los administradores de la base de datos. **8.7.d** Revise los parámetros de control de acceso de la base de datos, los parámetros de configuración de la aplicación de la base de datos y las ID de aplicaciones relacionadas para verificar que solo las aplicaciones pueden usar las ID de la aplicación (y no los usuarios u otros procesos).
8.8 Asegúrese de que las políticas de seguridad y los procedimientos operativos de identificación y autenticación estén documentados, implementados y que sean de conocimiento para todas las partes afectadas. **8.8** Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos de identificación y autenticación cumplen con lo siguiente: · Estén documentados, · Estén en uso, y · Sean de conocimiento para todas las partes afectadas.
9.1 Utilice controles de entrada a la empresa apropiados para limitar y supervisar el acceso físico a los sistemas en el entorno de datos del titular de la tarjeta. **9.1** Verifique la existencia de controles de seguridad física para cada sala de informática, centro de datos y otras áreas físicas con sistemas en el entorno de datos del titular de la tarjeta. · Verifique que se controle el acceso con lectores de placas de identificación u otros dispositivos, incluidas placas autorizadas y llave y candado. · Observe un intento de algún administrador del sistema para iniciar sesión en las consolas de sistemas seleccionados de forma aleatoria en un entorno de datos del titular de la tarjeta y verifique que estén “aseguradas” y se impida el uso no autorizado.
9.1.1 Utilice cámaras de video u otros mecanismos de control de acceso (o ambos) para supervisa **9.1.1.a** Verifique que las cámaras de video u otros mecanismos de control de acceso (o ambos) se usen para supervisar los puntos de entrada y salida de áreas confidenciales. **9.1.1.b** Verifique que las cámaras de video u otros mecanismos de control de acceso (o ambos) estén protegidos contra alteraciones o desactivaciones. **9.1.1.c** Verifique que se controlen las cámaras de video u otros mecanismos de control de acceso, y que los datos de dichas cámaras o mecanismos se almacenen, al menos, durante tres meses el acceso físico de personas a áreas confidenciales. Revise los datos recopilados y correlaciónelos con otras entradas. Guárdelos durante al menos tres meses, a menos que la ley estipule lo contrario.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
9.1.2 Implemente controles físicos o lógicos para restringir el acceso a conexiones de red de acceso público. **9.1.2** Entreviste al personal responsable y observe las ubicaciones de las conexiones de red de acceso público para verificar que se implementen controles físicos o lógicos a fin de restringir el acceso a las conexiones de red de acceso público.
9.1.3 Limite el acceso físico a los puntos de acceso inalámbricos, gateways, dispositivos manuales, hardware de redes o comunicaciones y líneas de telecomunicaciones. **9.1.3** Verifique que se restrinja correctamente el acceso físico a los puntos de acceso inalámbricos, gateways, dispositivos manuales, hardware de redes o comunicaciones y líneas de telecomunicaciones.
9.2 Desarrolle procedimientos que permitan distinguir, fácilmente, a los empleados y a los visitantes, de la siguiente manera: · Identificar empleados o visitantes nuevos (por ejemplo, mediante la asignación de placas). · Cambios en los requisitos de acceso. · Revocar las identificaciones de empleados cesantes y las identificaciones vencidas de visitantes (p. ej., placas de identificación). **9.2.a** Revise los procesos documentados para verificar que los procedimientos se definan de manera tal que se pueda realizar una identificación y distinción entre empleados y visitantes. · Verifique que los procesos incluyan lo siguiente: · Identificar empleados o visitantes nuevos (por ejemplo, mediante la asignación de placas). · Cambiar los requisitos de acceso. · Revocar las identificaciones de empleados cesantes y las identificaciones vencidas de visitantes (p. ej., placas de identificación). **9.2.b** Observe los procesos para identificar y distinguir entre empleados y visitantes, y verifique lo siguiente: · Los visitantes están claramente identificados. · Es fácil distinguir entre empleados y visitantes. **9.2.c** Verifique que el acceso al proceso de identificación (como el sistema de placas) esté limitado solo al personal autorizado.
9.3 Controle el acceso físico de los empleados a las áreas confidenciales de la siguiente manera: · El acceso se debe autorizar y basar en el trabajo de cada persona. · El acceso se debe cancelar inmediatamente después de finalizar el trabajo, y todos los mecanismos de acceso físico, como claves, tarjetas de acceso, se deben devolver o desactivar. **9.3.a** En el caso de un grupo de empleados con acceso físico a un área confidencial, entreviste al personal responsable y observe las listas de control de acceso para verificar lo siguiente: · El acceso al área confidencial está autorizado. · La persona necesita acceder para realizar su trabajo. **9.3.b** Observe el acceso del personal a un área confidencial, para verificar que todo el personal tenga autorización antes de que accedan. **9.3.c** Seleccione una muestra de empleados que hayan dejado de trabajar recientemente y revise las listas de control de acceso para verificar que no tenga acceso físico a un área confidencial.
9.4 Implemente procedimientos para identificar y autorizar a los visitantes. Los procedimientos deben incluir lo siguiente: **9.4** Verifique que los controles de acceso y las autorizaciones de los visitantes se implementen de la siguiente manera:

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
9.4.1 Los visitantes reciben autorización antes de ingresar en las áreas de procesamiento o almacenamiento de los datos del titular de la tarjeta y estarán acompañados en todo momento. **9.4.1.a** Observe los procedimientos y entreviste al personal para verificar que los visitantes reciben autorización antes de acceder a áreas de procesamiento o almacenamiento de los datos del titular de la tarjeta y que estén siempre acompañados. **9.4.1.b** Observe el uso de las placas para visitantes u otro tipo de identificación a fin de verificar que las placas de identificación física no permitan el acceso sin acompañantes a áreas físicas donde se procesan o conservan datos del titular de la tarjeta.
9.4.2 Se identifican los visitantes y se les entrega una placa u otro elemento de identificación con fecha de vencimiento y que permite diferenciar claramente entre empleados y visitantes. **9.4.2.a** Observe las personas dentro de las instalaciones para verificar que se usen placas para visitantes u otro tipo de identificación, y que los visitantes se puedan distinguir fácilmente de los empleados que trabajan en la empresa. **9.4.2.b** Verifique que las placas para visitantes y otro tipo de identificación tengan vencimiento.
9.4.3 Los visitantes deben entregar la placa o la identificación antes de salir de las instalaciones o al momento del vencimiento. **9.4.3**Observe la salida de los visitantes de las instalaciones para verificar que se solicite la entrega de su placa o de otro tipo de identificación al partir o al momento del vencimiento.
9.4.4 Se usa un registro de visitantes para llevar una pista de auditoría física de la actividad de los visitantes en las instalaciones, en las salas de informática y en los centros de datos donde se almacenan o se transmiten los datos del titular de la tarjeta. Documente el nombre del visitante, la empresa a la que representa y el empleado que autoriza el acceso físico en el registro. Conserve este registro durante tres meses como mínimo, a menos que la ley estipule lo contrario. **9.4.4.a** Verifique que se implemente un registro de visitantes para registrar el acceso físico a las instalaciones, así como también a las salas de informática y a los centros de datos donde se almacenan o transmiten los datos del titular de la tarjeta. **9.4.4.b** Verifique que el registro incluya lo siguiente: · Nombre del visitante · Empresa representada · Empleado que autoriza el acceso físico **9.4.4.c** Verifique que el registro se conserve durante, al menos, tres meses.
9.5 Proteja físicamente todos los medios. **9.5** Verifique que los procedimientos para proteger los datos del titular de la tarjeta incluyan controles para el resguardo seguro de todos los medios (entre otros, computadoras, dispositivos electrónicos extraíbles, recibos e informes en papel y faxes).
9.5.1 Almacene los medios de copias de seguridad en un lugar seguro, preferentemente, en un lugar externo a la empresa, como un centro alternativo o para copias de seguridad, o en un centro de almacenamiento comercial. Revise la seguridad de dicho lugar una vez al año como mínimo. **9.5.1** Verifique que el lugar de almacenamiento se revise una vez al año al menos para determinar que el almacenamiento de medios de copia de seguridad sea seguro.
9.6 Lleve un control estricto de la distribución interna o externa de todos los tipos de medios y realice lo siguiente: **9.6** Verifique que exista una política para controlar la distribución de medios y que dicha política abarque todos los medios distribuidos, incluso los que se distribuyen a personas.
9.6.1 Clasifique los medios para poder determinar la confidencialidad de los datos. **9.6.1** Verifique que todos los medios se hayan clasificado para poder determinar la confidencialidad de los datos.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
9.6.2 Envíe los medios por correo seguro u otro método de envío que se pueda rastrear con precisión. **9.6.2.a** Entreviste al personal y revise los registros para verificar que todos los medios enviados fuera de la empresa estén registrados y se envíen por correo seguro u otro método de envío que se pueda rastrear. **9.6.2.b** Seleccione una muestra actual de varios días de registros de seguimiento externos de todos los medios y verifique que se documenten los detalles de seguimiento.
9.6.3 Asegúrese de que la gerencia apruebe todos y cada uno de los medios que se trasladen desde un área segura (incluso, cuando se distribuyen los medios a personas). **9.6.3** Seleccione una muestra actual de varios días de registros de seguimiento externos de todos los medios. Mediante la evaluación de los registros y las entrevistas al personal responsable, verifique que se cuente con la debida autorización de la gerencia cuando sea necesario trasladar los medios desde un área segura (incluso, cuando los medios se distribuyen a personas).
9.7 Lleve un control estricto del almacenamiento y la accesibilidad de los medios. **9.7**Obtenga y revise la política para controlar el almacenamiento y el mantenimiento de todos los medios y verifique que la política requiera inventarios periódicos de medios.
9.7.1 Lleve un registro detallado del inventario de todos los medios y lleve a cabo inventarios de los medios, al menos, una vez al año. **9.7.1** Revise los registros de inventarios de los medios para verificar que se conserven los registros y que se lleven a cabo inventarios de medios, al menos, una vez al año.
9.8 Destruya los medios cuando ya no sea necesario guardarlos por motivos comerciales o legales de la siguiente manera: **9.8** Revise periódicamente la política de destrucción de medios y verifique que abarque todos los medios y que defina requisitos para lo siguiente: · Los materiales de copias en papel se deben cortar en tiras, incinerarse o convertirse en pulpa para tener la certeza de que no podrán reconstruirse. · Los contenedores de almacenamiento que se usan para los materiales que se destruirán deben estar protegidos. · Los datos del titular de la tarjeta en los medios electrónicos deben quedar irrecuperables (por ejemplo, a través de un programa con la función de borrado seguro según las normas aceptadas en la industria para lograr una eliminación segura o mediante la destrucción física de los medios).
9.8.1 Corte en tiras, incinere o convierta en pulpa los materiales de copias en papel para que no se puedan reconstruir los datos del titular de la tarjeta. Proteja los contenedores de almacenamiento destinados a los materiales que se destruirán. **9.8.1.a** Entreviste al personal y revise los procedimientos para verificar que los materiales de copias en papel se corten en tiras, se incineren o se conviertan en pulpa para tener la certeza de que no podrán reconstruirse. **9.8.1.b** Revise los contenedores de almacenamiento utilizados para los materiales que se destruirán y verifique que dichos contenedores estén asegurados.
9.8.2 Controle que los datos del titular de la tarjeta guardados en medios electrónicos sean irrecuperables para que no se puedan reconstruir. **9.8.2** Verifique que los datos del titular de la tarjeta guardados en dispositivos electrónicos sean irrecuperables (por ejemplo, a través de un programa con la función de borrado seguro según las normas aceptadas en la industria para lograr una eliminación segura o mediante la destrucción física de los medios).
9.9 Proteja los dispositivos que capturan datos de tarjetas de pago mediante la interacción física directa con la tarjeta para proporcionar protección contra alteraciones y sustituciones. **9.9** Revise las políticas y los procedimientos documentados para verificar que se realice lo siguiente: · Conservar una lista de los dispositivos. · Inspeccionar los dispositivos periódicamente para buscar intentos de alteración o sustitución. · Capacitar al personal para que detecten comportamientos sospechosos e informen la alteración o sustitución de dispositivos.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
9.9.1 Lleve una lista actualizada de los dispositivos. La lista debe incluir lo siguiente: · Marca y modelo del dispositivo · Ubicación del dispositivo (por ejemplo, la dirección de la empresa o de la instalación donde se encuentra el dispositivo) · Número de serie del dispositivo u otro método de identificación única **9.9.1.a** Revise la lista de los dispositivos y verifique que incluya lo siguiente: · Marca y modelo del dispositivo · Ubicación del dispositivo (por ejemplo, la dirección de la empresa o de la instalación donde se encuentra el dispositivo) · Número de serie del dispositivo u otro método de identificación única **9.9.1.b** Seleccione una muestra de dispositivos de la lista y observe la ubicación del dispositivo para verificar que la lista sea exacta y esté actualizada. **9.9.1.c** Entreviste al personal para verificar que la lista de dispositivos se actualice cuando se agreguen, reubiquen, desactiven, etc., dispositivos.
9.9.2 Inspeccione periódicamente la superficie de los dispositivos para detectar alteraciones (por ejemplo, incorporación de componentes de duplicación de datos en el dispositivo) o sustituciones (por ejemplo, controle el número de serie u otras características del dispositivo para verificar que no se haya cambiado por un dispositivo fraudulento). **9.9.2.a** Revise los procedimientos documentados para verificar que estén definidos para incluir lo siguiente: · Procedimientos para inspeccionar los dispositivos · Frecuencia de las inspecciones **9.9.2.b** Entreviste al personal responsable y observe los procesos de inspección para verificar lo siguiente: · El personal conoce los procedimientos para inspeccionar los dispositivos. · Todos los dispositivos se inspeccionan periódicamente para buscar indicios de alteraciones y sustitución.
9.9.3 Capacite al personal para que detecten indicios de alteración o sustitución en los dispositivos. La capacitación debe abarcar lo siguiente: · Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de autorizarlos a acceder y modificar un dispositivo o solucionar algún problema. · No instalar, cambiar ni devolver dispositivos sin verificación. · Estar atentos a comportamientos sospechosos cerca del dispositivo (por ejemplo, personas desconocidas que intentan desconectar o abrir el dispositivo). · Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por ejemplo, a un gerente o encargado de seguridad). **9.9.3.a** Revise el material de capacitación para el personal que trabaja en los puntos de venta para verificar que, en la capacitación, se incluya lo siguiente: · Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de otorgarles autorización para acceder y modificar un dispositivo o solucionar algún problema. · No instalar, cambiar ni devolver dispositivos sin verificación. · Estar atentos a comportamientos sospechosos cerca del dispositivo (por ejemplo, personas desconocidas que intentan desconectar o abrir el dispositivo). · Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por ejemplo, a un gerente o encargado de seguridad).

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
9.9.3.b Entreviste a un grupo del personal del punto de venta para verificar que hayan recibido capacitación y que conozcan los procedimientos para realizar lo siguiente: · Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de otorgarles autorización para acceder y modificar un dispositivo o solucionar algún problema. · No instalar, cambiar ni devolver dispositivos sin verificación. · Estar atentos a comportamientos sospechosos cerca del dispositivo (por ejemplo, personas desconocidas que intentan desconectar o abrir el dispositivo). · Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por ejemplo, a un gerente o encargado de seguridad).
9.10 Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso físico a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas. **9.10** Revise la documentación, entreviste al personal y verifique que las políticas de seguridad y los procedimientos operativos para restringir el acceso físico a los datos del titular de la tarjeta cumplan con lo siguiente: · Estén documentados, · Estén en uso, y · Sean de conocimiento para todas las partes afectadas.
10.1 Implemente pistas de auditoría para vincular todo acceso a componentes del sistema con usuarios específicos. **10.1** Verifique, mediante la observación y entrevistas al administrador del sistema, que se realice lo siguiente: · Las pistas de auditoría deben estar habilitadas y activas para los componentes del sistema. · El acceso a los componentes del sistema debe estar vinculado a usuarios específicos.
10.2 Implemente pistas de auditoría automáticas en todos los componentes del sistema a fin de reconstruir los siguientes eventos: **10.2** Entreviste al personal responsable, observe los registros de auditoría, revise la configuración de los registros de auditoría y realice lo siguiente:
10.2.1 Todo acceso por parte de usuarios a los datos del titular de la tarjeta. **10.2.1** Verifique que se registre todo acceso de los usuarios a los datos del titular de la tarjeta.
10.2.2 Todas las acciones realizadas por personas con privilegios de raíz o administrativos **10.2.2** Verifique que se registren todas las acciones que realizan personas con privilegios administrativos o de raíz.
10.2.3 Acceso a todas las pistas de auditoría **10.2.3** Verifique que se registre el acceso a todas las pistas de auditoría.
10.2.4 Intentos de acceso lógico no válidos **10.2.4** Verifique que se registren los intentos de acceso lógico no válidos.
10.2.5 Uso y cambios de los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y el aumento de privilegios, y de todos los cambios, incorporaciones y eliminaciones de las cuentas con privilegios administrativos o de raíz. **10.2.5.a** Verifique que se registre el uso de los mecanismos de identificación y autenticación. **10.2.5.b** Verifique que se registre todo aumento de privilegios. **10.2.5.c** Verifique que se registren todos los cambios, incorporaciones y eliminaciones de cualquier cuenta con privilegios administrativos o de raíz.
10.2.6 Inicialización, detención o pausa de los registros de auditoría **10.2.6** Verifique que se registre lo siguiente: · Inicialización de los registros de auditoría. · Detención o pausa de los registros de auditoría.
10.2.7 Creación y eliminación de objetos en el nivel del sistema **10.2.7** Verifique que estén registradas la creación y la eliminación de objetos en el nivel del sistema.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
10.3 Registre, al menos, las siguientes entradas de pistas de auditoría de los componentes del sistema para cada evento: **10.3.1** Identificación de usuarios **10.3.1** Verifique que la identificación de usuario se incluya en las entradas del registro. **10.3.2** Tipo de evento **10.3.2** Verifique que el tipo de evento se incluya en las entradas del registro. **10.3.3** Fecha y hora. **10.3.3** Verifique que el sello de fecha y hora se incluya en las entradas del registro. **10.3.4** Indicación de éxito o fallo **10.3.4** Verifique que la indicación de éxito o fallo se incluya en las entradas del registro. **10.3.5** Origen del evento **10.3.5** Verifique que el origen del evento se incluya en las entradas del registro. **10.3.6** Identidad o nombre de los datos, componentes del sistema o recursos afectados. **10.3.6** Verifique que la identidad o el nombre de los datos, de los componentes del sistema o de los recursos afectados se incluyan en las entradas del registro. **10.4** Utilizando tecnología de sincronización, sincronice todos tiempos y relojes críticos y asegúrese de que lo siguiente sea implementado para adquirir, distribuir y almacenar tiempos. **10.4** Revise las normas de configuración y los procesos para verificar que la tecnología de sincronización se implemente y mantenga actualizada, según los Requisitos 6.1 y 6.2 de las PCI DSS.
10.4.1 Los sistemas críticos tienen un horario uniforme y correcto. **10.4.1.a** Revise el proceso para adquirir, distribuir y guardar el horario correcto en la organización para verificar lo siguiente: · Solo los servidores de horario central designados deben recibir señales de tiempo de fuentes externas, y las señales de tiempo de fuentes externas se deben basar en la hora atómica internacional o UTC. · Si hubiera más de un servidor de horario designado, estos se emparejan para mantener la hora exacta. · Los sistemas reciben información horaria solo de los servidores de horario central designados. **10.4.1.b** Observe la configuración de los parámetros del sistema relacionados con la hora para obtener una muestra de los componentes del sistema y verificar lo siguiente: · Solo los servidores de horario central designados deben recibir señales de tiempo de fuentes externas, y las señales de tiempo de fuentes externas se deben basar en la hora atómica internacional o UTC. · Si hubiera más de un servidor de horario designado, estos se emparejan para mantener la hora exacta. · Los sistemas reciben información horaria solo de los servidores de horario central designados.
10.4.2 Los datos de tiempo están protegidos. **10.4.2.a** Revise la configuración del sistema y los parámetros de configuración de sincronización para verificar que el acceso a los datos de la hora esté limitado solo al personal que tenga una necesidad comercial para acceder a los datos de la hora. **10.4.2.b** Revise la configuración del sistema, los registros y parámetros de configuración de sincronización y los procesos para verificar que todos los cambios en la configuración de la hora en los sistemas críticos se registren, supervisen y revisen.
10.4.3 Los parámetros de la hora se reciben de fuentes aceptadas por la industria. **10.4.3** Revise la configuración del sistema para verificar que los servidores de horario acepten actualizaciones de hora de fuentes externas específicas aceptadas por la industria (para evitar que personas malintencionadas cambien el reloj). De forma opcional, se pueden cifrar estas actualizaciones con una clave simétrica, y se pueden crear listas de control de acceso que especifiquen las direcciones IP de equipos cliente a los que se proporcionarán las actualizaciones de tiempo (para evitar el uso no autorizado de servidores de hora internos).

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
10.5 Proteja las pistas de auditoría para que no se puedan modificar. **10.5** Entreviste a los administradores del sistema y revise los permisos y la configuración del sistema para verificar que las pistas de auditoría sean seguras y que no se puedan modificar de la siguiente manera:
10.5.1 Limite la visualización de las pistas de auditoría a quienes lo necesiten por motivos laborales. **10.5.1** Solo aquellas personas que lo necesiten por motivos laborales pueden visualizar los archivos de las pistas de auditoría.
10.5.2 Proteja los archivos de las pistas de auditoría contra modificaciones no autorizadas. **10.5.2** Verifique que los archivos actuales de las pistas de auditoría estén protegidos contra modificaciones no autorizadas a través de mecanismos de control de acceso y la segregación física o de redes.
10.5.3 Realice copias de seguridad de los archivos de las pistas de auditoría de manera oportuna en medios o servidores de registros centralizados que sean difíciles de modificar. **10.5.3** Se realiza, oportunamente, una copia de seguridad de los archivos actuales de las pistas de auditoría en medios o servidores de registros centralizados que son difíciles de modificar.
10.5.4 Elabore registros para tecnologías externas en un dispositivo de medios o un servidor de registros interno, seguro y centralizado. **10.5.4** Los registros para tecnologías externas (por ejemplo, tecnologías inalámbricas, firewalls, DNS, correo) se copian en medios o servidores de registros centralizados, internos y seguros.
10.5.5 Utilice el software de supervisión de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas (aunque el hecho de agregar nuevos datos no deba generar una alerta). **10.5.5** Revise la configuración del sistema, los archivos monitoreados y los resultados de las actividades de supervisión para corroborar el uso del software de supervisión de integridad de archivos o de detección de cambios en los registros.
10.6 Revise los registros y los eventos de seguridad en todos los componentes del sistema para identificar anomalías o actividades sospechosas. Nota: Se pueden usar herramientas de recolección, análisis y alerta de registros. **10.6.1** Revise las siguientes opciones, al menos, una vez al día: · Todos los eventos de seguridad. · Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD · Registros de todos los componentes críticos del sistema. · Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, firewalls, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención], servidores de autenticación, servidores de redireccionamiento de comercio electrónico, etc.). **10.6.1.a** Revise las políticas y los procedimientos de seguridad para verificar que los procedimientos se definen para revisar lo siguiente, al menos, una vez al día, ya sea manualmente o con herramientas de registro: · Todos los eventos de seguridad. · Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD · Registros de todos los componentes críticos del sistema. · Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, firewalls, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención], servidores de autenticación, servidores de redireccionamiento de comercio electrónico, etc.).

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
10.6.1.b Observe los procesos y entreviste al personal para verificar que los siguientes puntos se controlen, al menos, una vez al día: · Todos los eventos de seguridad. · Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD · Registros de todos los componentes críticos del sistema. · Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, firewalls, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención], servidores de autenticación, servidores de redireccionamiento de comercio electrónico, etc.).
10.6.2 Revise los registros de todos los demás componentes del sistema periódicamente, de conformidad con la política y la estrategia de gestión de riesgos de la organización y según lo especificado en la evaluación anual de riesgos de la organización. **10.6.2.a** Revise las políticas y los procedimientos de seguridad para verificar que estén definidos para realizar una revisión periódica de los registros de todos los demás componentes del sistema, ya sea de forma manual o con herramientas de registros, según la política y estrategia de gestión de riesgos de la organización. **10.6.2.b** Revise la documentación de evaluación de riesgos de la organización y entreviste al personal para verificar que las revisiones se realicen en conformidad con las políticas y la estrategia de gestión de riesgos de la organización.
10.6.3 Realice un seguimiento de las excepciones y anomalías detectadas en el proceso de revisión. **10.6.3.a** Revise las políticas y los procedimientos de seguridad para verificar que los procesos se definen para realizar un seguimiento de las excepciones y anomalías detectadas en el proceso de revisión. **10.6.3.b** Observe los procesos y entreviste al personal para verificar que se realice un seguimiento de las excepciones y anomalías.
10.7 Conserve el historial de pistas de auditorías durante, al menos, un año, con un mínimo de disponibilidad para análisis de tres meses (por ejemplo, en línea, archivados o recuperables para la realización de copias de seguridad). **10.7.a** Revise las políticas y los procedimientos de seguridad y verifique que definan lo siguiente: · Políticas de retención de registros de auditoría · Procedimientos para conservar los registros de auditoría durante, al menos, un año, con un mínimo de disponibilidad en línea de tres meses. **10.7.b** Entreviste al personal y revise los registros de auditoría para verificar que estén disponible durante, al menos, un año. **10.7.c** Entreviste al personal y observe los procesos para verificar que se puedan recuperar, al menos, los registros de los últimos tres meses para analizarlos.
10.8 Requisitos adicionales solo para los proveedores de servicios: Implementar un proceso para la detección oportuna y la presentación de informes de fallas de los sistemas críticos de control de seguridad, incluido, pero no limitado a la falla de: · Firewalls · IDS/IPS · FIM · Antivirus · Controles de acceso físicos · Controles de acceso lógico · Mecanismos de registro de auditoría · Controles de segmentación (si se utilizan)

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
10.8.a Revise las políticas y los procedimientos documentados para verificar que estén definidos los procesos de detección oportuna y presentación de informes de las fallas de los sistemas críticos de control de seguridad, que incluyan entre otras fallas por: · Firewalls · IDS/IPS · FIM · Antivirus · Controles de acceso físicos · Controles de acceso lógico · Mecanismos de registro de auditoría · Controles de segmentación (si se utilizan) **10.8.b** Revise los procesos de detección y de alerta y entreviste al personal para verificar que los procesos se implementan para todos los controles de seguridad críticos, y que la falla de un control de seguridad críticos da lugar a la generación de una alerta.
10.8.1 Requisitos adicionales solo para los proveedores de servicios: Responder a las fallas de los controles de seguridad críticos en el momento oportuno. Los procesos para responder en caso de fallas en el control de seguridad son los siguientes: · Restaurar las funciones de seguridad · Identificar y documentar la duración (fecha y hora de inicio a fin) de la falla de seguridad · Identificar y documentar las causas de la falla, incluida la causa raíz, y documentar la remediación requerida para abordar la causa raíz · Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad. · Realizar una evaluación de riesgos para determinar si se requieren más acciones como resultado de la falla de seguridad · Implementar controles para prevenir que se vuelva a producir la causa de la falla · Reanudar la supervisión de los controles de seguridad **Nota:** Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito. **10.8.1.a** Revise las políticas y procedimientos documentados y entreviste al personal para verificar que los procesos están definidos e implementados para responder a una falla del control de seguridad, e incluya: · Restaurar las funciones de seguridad · Identificar y documentar la duración (fecha y hora de inicio a fin) de la falla de seguridad · Identificar y documentar las causas de la falla, incluida la causa raíz, y documentar la remediación requerida para abordar la causa raíz · Identificar y abordar cualquier problema de seguridad que surja durante la falla. · Realizar una evaluación de riesgos para determinar si se requieren más acciones como resultado de la falla de seguridad · Implementar controles para prevenir que se vuelva a producir la causa de la falla · Reanudar la supervisión de los controles de seguridad **10.8.1.b** Revise los registros para verificar que se documentan las fallas del control de seguridad para incluir: · Identificación de las causas de la falla, incluida la causa raíz · Duración (fecha y hora de inicio y fin) de la falla de seguridad · Detalles de la remediación necesaria para abordar la causa raíz

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
10.9 Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear todos los accesos a los recursos de la red y a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas. **10.9** Revise la documentación, entreviste al personal y verifique que las políticas de seguridad y los procedimientos operativos para monitorear todos los accesos a los recursos de la red y a los datos del titular de la tarjeta cumplan con lo siguiente: · Estén documentados, · Estén en uso, y · Sean de conocimiento para todas las partes afectadas.
11.1 Implemente procesos para determinar la presencia de puntos de acceso inalámbrico (802.11), detecte e identifique, trimestralmente, todos los puntos de acceso inalámbricos autorizados y no autorizados. Nota: Los métodos que se pueden utilizar en este proceso incluyen, entre otros, análisis de redes inalámbricas, inspecciones lógicas/físicas de los componentes y de la infraestructura del sistema, NAC (control de acceso a la red) o IDS/IPS (sistemas de intrusión-detección y sistemas de intrusión-prevención) inalámbricos. Independientemente de los métodos utilizados, deben ser suficientes para detectar e identificar tanto los dispositivos no autorizados como los autorizados. **11.1.a** Revise las políticas y los procedimientos para verificar que los procesos estén definidos para detectar e identificar, trimestralmente, puntos de acceso inalámbricos autorizados y no autorizados. **11.1.b** Verifique que la metodología sea la adecuada para detectar e identificar cualquier punto de acceso inalámbrico no autorizado, que incluya, al menos, lo siguiente: · Tarjetas WLAN insertadas en los componentes del sistema · Dispositivos portátiles o móviles conectados a los componentes del sistema para crear puntos de acceso inalámbricos (por ejemplo, mediante USB, etc.). · Dispositivos inalámbricos conectados a un puerto o a un dispositivo de red. **11.1.c** Si se realiza un análisis inalámbrico, revise el resultado de los últimos análisis inalámbricos para verificar lo siguiente: · Se identifican los puntos de acceso inalámbricos autorizados y no autorizados. · El análisis se realiza, al menos, trimestralmente en todos los componentes del sistema y en todas las instalaciones. **11.1.d** Si se utiliza la supervisión automatizada (por ejemplo, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención] inalámbricos, NAC [control de acceso a la red], etc.), verifique que la configuración genere alertas para notificar al personal.
11.1.1 Lleve un inventario de los puntos de acceso inalámbricos autorizados que incluyan una justificación comercial documentada. **11.1.1** Revise los registros documentados para verificar que se conserve un inventario de los puntos de acceso inalámbricos autorizados y que se documente una justificación comercial para todos los puntos de acceso inalámbricos autorizados.
11.1.2 Implemente procedimientos de respuesta a incidentes en caso de que se detecten puntos de acceso inalámbricos no autorizados. **11.1.2.a** Revise el plan de respuesta a incidentes de la organización (Requisito 12.10) para verificar que defina y solicite una respuesta en caso de detectar puntos de acceso inalámbricos no autorizados. **11.1.2.b** Entreviste al personal responsable e inspeccione los análisis inalámbricos recientes y las respuestas correspondientes para verificar que se tomen medidas cuando se encuentren puntos de acceso inalámbricos no autorizados.
11.2 Realice análisis internos y externos de las vulnerabilidades de la red, al menos, trimestralmente y después de cada cambio significativo en la red (como por ejemplo, la instalación de nuevos componentes del sistema, cambios en la topología de la red, modificaciones en las normas de firewall, actualizaciones de productos). **11.2** Revise los informes de análisis y la documentación de respaldo para verificar que se realicen análisis de las vulnerabilidades internas y externas de la siguiente manera:

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
11.2.1 Realice análisis interno de vulnerabilidades trimestralmente. Aborde las vulnerabilidades y realice redigitalizaciones para verificar que todas las vulnerabilidades de "alto riesgo" se resuelven de acuerdo con la clasificación de la vulnerabilidad de la entidad (según el Requisito 6.1). Los análisis deben estar a cargo de personal calificado. **11.2.1.a** Revise los informes de análisis y verifique que se hayan realizado cuatro análisis trimestrales internos en los últimos 12 meses. **11.2.1.b** Revise los informes de los análisis y verifique que el proceso incluya la repetición de los análisis hasta que se corrijan todas las vulnerabilidades “de alto riesgo”, según las disposiciones del Requisito 6.1 de las PCI DSS. **11.2.1.c** Entreviste al personal para verificar que el análisis lo haya realizado un recurso interno calificado o personal externo capacitado, y si corresponde, que la persona que realice la prueba sea independiente de la empresa (no es necesario que sea un QSA o ASV).
11.2.2 Los análisis trimestrales de vulnerabilidades externas deben estar a cargo de un ASV (proveedor aprobado de escaneo) que esté certificado por el PCI SSC (PCI Security Standards Council). Vuelva a realizar los análisis cuantas veces sea necesario hasta que todos los análisis estén aprobados. **Nota:** Los análisis trimestrales de vulnerabilidades externas debe realizarlos un Proveedor aprobado de análisis (ASV) certificado por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC). **11.2.2.a** Revise los resultados de los últimos cuatro análisis trimestrales de vulnerabilidades externas y verifique que se hayan realizado cuatro análisis trimestrales de vulnerabilidades externas en los últimos 12 meses. **11.2.2.b** Revise los resultados de cada análisis trimestral y repita los análisis para verificar que se hayan cumplido los requisitos de la Guía del programa de ASV (proveedor aprobado de escaneo) para obtener un análisis aprobado (por ejemplo, que no haya vulnerabilidades con una puntuación CVSS de 4.0 o superior y que no haya fallas automáticas). **11.2.2.c** Revise los informes de análisis para verificar que los haya realizado un ASV (proveedor aprobado de escaneo) que esté certificado por el PCI SSC.
11.2.3 Lleve a cabo análisis internos y externos, y repítalos, según sea necesario, después de realizar un cambio significativo. Los análisis deben estar a cargo de personal calificado. **11.2.3.a** Inspeccione y coteje la documentación del control de cambios y los informes de análisis para verificar que se hayan analizado los componentes del sistema que hayan tenido cambios significativos. **11.2.3.b** Revise los informes de los análisis y verifique que el proceso de análisis incluye la repetición de los análisis hasta que: · No se hayan registrado vulnerabilidades con puntuaciones CSVV de 4.0 o superior en análisis externos. · Se hayan corregido todas las vulnerabilidades “de alto riesgo”, según lo estipulado en el Requisito 6.1 de las PCI DSS, en los análisis internos. 11.2.3.c Verifique que el análisis lo haya realizado un recurso interno calificado o personal externo capacitado, y si corresponde, que la persona que realiza la prueba sea independiente de la empresa (no es necesario que sea un QSA o ASV).

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
11.3 Implemente una metodología para las pruebas de penetración que incluya lo siguiente: · Esté basada en los enfoques de pruebas de penetración aceptados por la industria (por ejemplo, NIST SP800- 115). · Incluya cobertura de todo el perímetro del CDE (entorno de datos del titular de la tarjeta) y de los sistemas críticos. · Incluya pruebas del entorno interno y externo de la red. · Incluya pruebas para validar cualquier segmentación y controles de reducción del alcance. · Defina las pruebas de penetración de la capa de la aplicación para que incluyan, al menos, las vulnerabilidades enumeradas en el Requisito 6.5. · Defina las pruebas de penetración de la capa de la red para que incluyan los componentes que admiten las funciones de red y los sistemas operativos. · Incluya la revisión y evaluación de las amenazas y vulnerabilidades ocurridas en los últimos 12 meses. · Especifique la retención de los resultados de las pruebas de penetración y los resultados de las actividades de corrección. **11.3** Revise la metodología de pruebas de penetración y entreviste al personal responsable para verificar que se implemente la metodología e incluya lo siguiente: · Esté basada en los enfoques de pruebas de penetración aceptados por la industria (por ejemplo, NIST SP800- 115). · Incluya cobertura de todo el perímetro del CDE (entorno de datos del titular de la tarjeta) y de los sistemas críticos. · Incluya pruebas del entorno interno y externo de la red. · Incluya pruebas para validar cualquier segmentación y controles de reducción del alcance. · Defina las pruebas de penetración de la capa de la aplicación para que incluyan, al menos, las vulnerabilidades enumeradas en el Requisito 6.5. · Defina las pruebas de penetración de la capa de la red para que incluyan los componentes que admiten las funciones de red y los sistemas operativos. · Incluya la revisión y evaluación de las amenazas y vulnerabilidades ocurridas en los últimos 12 meses. · Especifique la retención de los resultados de las pruebas de penetración y los resultados de las actividades de corrección.
11.3.1 Lleve a cabo pruebas de penetración externas, al menos, una vez al año y después de implementar una actualización o modificación significativa en las infraestructuras o aplicaciones (como, por ejemplo, actualizar el sistema operativo, agregar una subred o un servidor web al entorno). **11.3.1.a** Revise el alcance del trabajo y los resultados de la última prueba de penetración externa para verificar que se realice de la siguiente manera: · Según la metodología definida. · Por lo menos, anualmente · Después de cualquier cambio significativo en el entorno. **11.3.1.b** Verifique que la prueba la haya realizado un recurso interno calificado o un empleado externo capacitado, y si corresponde, que la persona que realiza la prueba sea independiente de la empresa (no es necesario que sea un QSA o ASV).

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
11.3.2.b Verifique que la prueba la haya realizado un recurso interno calificado o un empleado externo capacitado, y si corresponde, que la persona que realiza la prueba sea independiente de la empresa (no es necesario que sea un QSA o ASV).
11.3.3 Las vulnerabilidades de seguridad detectadas en las pruebas de penetración se corrigen, y las pruebas se repiten para verificar las correcciones. **11.3.3** Revise los resultados de las pruebas de penetración para verificar que se hayan corregido las vulnerabilidades de seguridad detectadas y que la repetición de las pruebas confirme que las vulnerabilidades se corrigieron.
11.3.4 Si se usa la segmentación para aislar el CDE (entorno de datos del titular de la tarjeta) de otras redes, realice pruebas de penetración, al menos, una vez al año y después de implementar cambios en los métodos o controles de **11.3.4.a** Revise los controles de segmentación y revise la metodología de las pruebas de penetración para verificar que los procedimientos estén definidos para comprobar todos los métodos de segmentación y confirmar que son operativos y eficaces, y que, además, aíslan todos los sistemas fuera de alcance de los sistemas en el CDE. **11.3.4.b** Examinar los resultados de la prueba de penetración más reciente para verificar que: · La prueba de penetración para verificar los controles de segmentación se realiza, al menos, una vez al año y después de cualquier cambio en los controles o métodos de segmentación. · La prueba de penetración abarca todos los controles o métodos de segmentación implementados. · La prueba de penetración verifica que los métodos de segmentación sean operativos y eficaces, y que aíslan todos los sistemas fuera de alcance de los sistemas dentro del CDE. **11.3.4.c** Verifique que la prueba la haya realizado un recurso interno capacitado o un empleado externo cualificado, y si corresponde, que la persona que realiza la prueba sea independiente de la empresa (no es necesario que sea un QSA o ASV).
11.3.4.1 Requisitos adicionales solo para los proveedores de servicios: Si se utiliza la segmentación, confirme el alcance de la PCI DSS al realizar pruebas de penetración en los controles de segmentación al menos cada seis meses, y después de cualquier cambio a los controles/métodos de segmentación. **11.3.4.1.a** Revise los resultados de la prueba de penetración más reciente para verificar que: · La prueba de penetración se realiza para verificar los controles de segmentación por lo menos cada seis meses y después de cualquier cambio a los controles/métodos de segmentación. · La prueba de penetración abarca todos los controles o métodos de segmentación implementados. · La prueba de penetración verifica que los métodos de segmentación sean operativos y eficaces, y que aíslan todos los sistemas fuera de alcance de los sistemas dentro del CDE. **11.3.4.1.b** Verifique que la prueba la haya realizado un recurso interno capacitado o un empleado externo cualificado, y si corresponde, que la persona que realiza la prueba sea independiente de la empresa (no es necesario que sea un QSA o ASV).
11.4 Use técnicas de intrusión-detección y de intrusión-prevención para detectar o prevenir intrusiones en la red. Monitoree todo el tráfico presente en el perímetro del entorno de datos del titular de la tarjeta y en los puntos críticos del entorno de datos del titular de la tarjeta, y alerte al personal ante la sospecha de riesgos. Mantenga actualizados todos los motores de intrusión-detección y de prevención, las bases y firmas. **11.4.a** Revise la configuración del sistema y los diagramas de red para verificar que se implementen técnicas (como los sistemas de intrusión-detección y de intrusión-prevención) para monitorear todo el tráfico en los siguientes lugares: · En el perímetro del entorno de datos del titular de la tarjeta. · En los puntos críticos del entorno de datos del titular de la tarjeta. **11.4.b** Revise la configuración del sistema y entreviste al personal responsable para confirmar que las técnicas de intrusión-detección y de intrusión-prevención alerten al personal de posibles riesgos. **11.4.c** Revise la configuración de las IDS/IPS (sistemas de intrusión-detección y sistemas de intrusión-prevención) y la documentación del proveedor para verificar que las técnicas de intrusión-detección y de intrusión-prevención se configuren, conserven y actualicen según las instrucciones del proveedor para garantizar una protección óptima.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
11.5 Implemente un mecanismo de detección de cambios (por ejemplo, herramientas de supervisión de integridad de archivos) para alertar al personal sobre modificaciones (incluyendo cambios, adiciones y eliminaciones) no autorizadas de archivos críticos del sistema, de archivos de configuración o de contenido, y configure el software para realizar comparaciones de archivos críticos, al menos, una vez por semana. Nota: A los fines de la detección de cambios, generalmente, los archivos críticos son aquellos que no se modifican con regularidad, pero cuya modificación podría implicar un riesgo o peligro para el sistema. **11.5.a** Verifique que se implemente el uso de un mecanismo de detección de cambios mediante la observación de la configuración del sistema y los archivos monitoreados, así como la revisión de los resultados de las actividades de supervisión. Ejemplos de archivos que se deben supervisar: · Ejecutables del sistema · Ejecutables de aplicaciones · Archivos de configuración y parámetros · Archivos de almacenamiento central, históricos o archivados, de registro y auditoría · Archivos críticos adicionales que determine la entidad (por ejemplo, a través de la evaluación de riesgos u otros medios) **11.5.b** Verifique que el mecanismo esté configurado para alertar al personal sobre modificaciones (incluyendo cambios, adiciones y eliminaciones) no autorizadas de archivos críticos, y para realizar comparaciones de archivos críticos, al menos, semanalmente.
11.5.1 Implemente un proceso para responder a las alertas que genera la solución de detección de cambios. **11.5.1** Entreviste al personal para verificar que todas las alertas se investiguen y resuelvan.
11.6 Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear y comprobar la seguridad estén documentados, implementados y que sean de conocimiento para todas las partes afectadas. **11.6** Revise la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos para monitorear y comprobar la seguridad cumplen con lo siguiente: · Estén documentados, · Estén en uso, y · Sean de conocimiento para todas las partes afectadas.
12.1 Establezca, publique, mantenga y distribuya una política de seguridad. **12.1** Examine la política de seguridad de la información y verifique que la política se publique y se distribuya a los usuarios del sistema que corresponda (incluidos proveedores, contratistas y socios de negocios).
12.1.1 Revise la política de seguridad, al menos, una vez al año y actualícela cuando se realicen cambios en el entorno. **12.1.1** Verifique que la política de seguridad de la información se revise, al menos, una vez al año y se actualice cuando sea necesario, de manera que refleje los cambios en los objetivos del negocio o en el entorno de riesgos.
12.2 Implemente un proceso de evaluación de riesgos que cumpla con lo siguiente: · Se realiza, al menos, una vez al año y después de implementar cambios significativos en el entorno (por ejemplo, adquisiciones, fusiones o reubicaciones, etc.). · Identifica activos críticos, amenazas y vulnerabilidades. · Los resultados en un análisis formal y documentado de riesgo. Los ejemplos de metodologías de evaluación de riesgos incluyen, entre otros, OCTAVE, ISO 27005 y NIST SP 800-30. **12.2.a** Verifique que se documenta un proceso anual de evaluación de riesgos que: · Identifica activos críticos, amenazas y vulnerabilidades. · Resultados en un análisis formal y documentado de riesgo **12.2.b** Revise la documentación de la evaluación de riesgos para verificar que el proceso de evaluación de riesgos se ejecute, al menos, una vez al año y después de cambios significativos en el entorno.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
12.3 Desarrolle políticas de uso para las tecnologías críticas y defina cómo usarlas correctamente. **12.3** Revise las políticas de uso de las tecnologías críticas y entreviste al personal responsable para verificar que se implementen las siguientes políticas y de la siguiente manera:
12.3.1 Aprobación explícita de las partes autorizadas **12.3.1** Verifique que las políticas de uso incluyan procesos para la aprobación explícita de partes autorizadas para utilizar las tecnologías.
12.3.2 Autenticación para el uso de la tecnología **12.3.2** Verifique que las políticas de uso incluyan procesos que autentiquen el uso de todas las tecnologías con ID de usuario y contraseña u otro elemento de autenticación (por ejemplo, token).
12.3.3 Lista de todos los dispositivos y el personal que tenga acceso **12.3.3** Verifique que las políticas de uso definen: · Una lista de todos los dispositivos críticos, y · Una lista del personal autorizado para utilizar los dispositivos.
12.3.4 Método para determinar, con exactitud y rapidez, el propietario, la información de contacto y el objetivo (por ejemplo, etiquetado, codificación o inventario de dispositivos). **12.3.4** Verifique que las políticas de uso definan un método para determinar, con exactitud y rapidez, el propietario, la información de contacto y el objetivo (por ejemplo, etiquetados, codificación o inventario de dispositivos).
12.3.5 Usos aceptables de la tecnología **12.3.5** Verifique que las políticas de uso definan los usos aceptables de la tecnología.
12.3.6 Ubicaciones aceptables de las tecnologías en la red **12.3.6** Verifique que las políticas de uso definan las ubicaciones aceptables de la tecnología en la red.
12.3.7 Lista de productos aprobados por la empresa **12.3.7** Verifique que las políticas de uso incluyan una lista de los productos aprobados por la empresa.
12.3.8 Desconexión automática de sesiones para tecnologías de acceso remoto después de un período específico de inactividad **12.3.8** Verifique que las políticas de uso requieran la desconexión automática de sesiones en las tecnologías de acceso remoto después de un período específico de inactividad. **12.3.8.b** Revise la configuración de las tecnologías de acceso remoto para verificar que las sesiones de acceso remoto se desconecten automáticamente después de un período específico de inactividad.
12.3.9 Activación de las tecnologías de acceso remoto para proveedores y socios de negocio sólo cuando sea necesario, con desactivación inmediata después de su uso **12.3.9** Verifique que las políticas de uso requieran la activación de las tecnologías de acceso remoto que usan los proveedores y socios comerciales solo cuando se necesiten y que se desactiven automáticamente después de usarlas.
12.3.10 En el caso del personal que tiene acceso a los datos del titular de la tarjeta mediante tecnologías de acceso remoto, prohíba copiar, mover y almacenar los datos del titular de la tarjeta en unidades de disco locales y en dispositivos electrónicos extraíbles, a menos que sea autorizado explícitamente para una necesidad comercial definida. Si existe una necesidad comercial autorizada, las políticas de uso deben disponer la protección de los datos de conformidad con los requisitos correspondientes de las PCI DSS. **12.3.10.a** Verifique que las políticas de uso prohíban copiar, mover o almacenar datos del titular de la tarjeta en unidades de disco locales y en dispositivos electrónicos extraíbles al acceder a dichos datos a través de tecnologías de acceso remoto. **12.3.10.b** En el caso del personal que cuenta con la autorización correcta, verifique que las políticas de uso dispongan que los datos del titular de la tarjeta se protejan de conformidad con los requisitos de las PCI DSS.
12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan, claramente, las responsabilidades de seguridad de la información de todo el personal. **12.4** Verifique que las políticas de seguridad de la información definan, con claridad, las responsabilidades de seguridad de la información de todo el personal.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
12.4.b Entreviste a un grupo de empleados responsables y verifique que comprendan las políticas de seguridad.
12.4.1 Requisitos adicionales solo para los proveedores de servicios: La gerencia ejecutiva deberá establecer la responsabilidad de la protección de los datos del titular de la tarjeta y un programa de cumplimiento de la PCI DSS para incluir: · Responsabilidad general de mantener el cumplimiento de la PCI DSS · Definir un estatuto para el programa de cumplimiento de la PCI DSS y la comunicación a la gerencia ejecutiva **12.4.1.a** Revise la documentación para verificar que la gerencia ejecutiva ha asignado la responsabilidad general de mantener el cumplimiento de la PCI DSS de la entidad. **12.4.1.b** Revise el estatuto de la PCI DSS de la empresa para verificar que se describen las condiciones en las que se organiza y se comunica a la gerencia ejecutiva el programa de cumplimiento de la PCI DSS.
12.5 Asigne a una persona o a un equipo las siguientes responsabilidades de administración de seguridad de la información: **12.5** Revise los procedimientos y las políticas de seguridad de la información para verificar lo siguiente: · La asignación formal de la seguridad de la información a un jefe de seguridad u a otro miembro de la gerencia relacionado con la seguridad. · Las siguientes responsabilidades de seguridad de la información se asignan de manera formal y específica:
12.5.1 Establezca, documente y distribuya las políticas y los procedimientos de seguridad. **12.5.1** Verifique que la responsabilidad de establecer, documentar y distribuir las políticas y los procedimientos de seguridad se asigne formalmente.
12.5.2 Monitoree y analice las alertas y la información de seguridad y comuníquelas al personal correspondiente. **12.5.2** Verifique que la responsabilidad de monitorear y analizar las alertas de seguridad y de distribuir la información al personal de las unidades comerciales y de seguridad se haya asignado formalmente.
12.5.3 Establezca, documente y distribuya los procedimientos de escalamiento y respuesta ante incidentes de seguridad para garantizar un manejo oportuno y efectivo de todas las situaciones. **12.5.3** Verifique que la responsabilidad de establecer, documentar y distribuir los procedimientos de escalamiento y de respuesta ante incidentes de seguridad se asigne formalmente.
12.5.4 Administre las cuentas de usuario, incluso las incorporaciones, eliminaciones y modificaciones. **12.5.4** Verifique que la responsabilidad de administrar (agregar, eliminar y modificar) las cuentas de usuario y la administración de la autenticación esté asignada formalmente.
12.5.5 Monitoree y controle todo acceso a los datos. **12.5.5** Verifique que la responsabilidad de monitorear y controlar todo acceso a los datos esté formalmente asignada.
12.6 Implemente un programa formal de concienciación sobre seguridad para que todo el personal tome conciencia de la importancia de la seguridad de los datos del titular de la tarjeta. **12.6.a** Revise el programa de concienciación sobre seguridad para verificar que ayuda a que todo el personal tome conciencia sobre la política y los procedimientos de seguridad de los datos del titular de la tarjeta. **12.6.b** Revise los procedimientos y la documentación del programa de concienciación sobre seguridad y realice lo siguiente:
12.6.1 Capacite al personal inmediatamente después de contratarlo y, al menos, una vez al año. Nota: Los métodos pueden variar según el rol del personal y del nivel de acceso a los datos del titular de la tarjeta. **12.6.1.a** Verifique que el programa de concienciación sobre seguridad proporcione diversos métodos para informar y educar a los empleados en lo que respecta a la concienciación (por ejemplo, carteles, cartas, notas, capacitación en línea, reuniones y promociones). **12.6.1.b** Verifique que el personal concurra a la capacitación de la concienciación sobre seguridad al ser contratados y, al menos, una vez al año.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
12.6.1.c Entreviste a un grupo de empleados para verificar que hayan realizado la capacitación de concienciación y que conozcan la importancia de la seguridad de los datos del titular de la tarjeta.
12.6.2 Exija al personal que realice, al menos, una vez al año, una declaración de que leyeron y entendieron la política y los procedimientos de seguridad de la empresa. **12.6.2** Verifique que el programa de concienciación sobre seguridad les exija a los empleados realizar, al menos, una vez al año, una declaración escrita o electrónica de que leyeron y entendieron la política de seguridad de la información de la empresa.
12.7 Examine al personal potencial antes de contratarlo a fin de minimizar el riesgo de ataques desde fuentes internas. (Entre los ejemplos de verificaciones de antecedentes se incluyen el historial de empleo, registro de antecedentes penales, historial crediticio y verificación de referencias). **12.7** Consulte con la gerencia del departamento de Recursos Humanos y verifique que se realiza un control de los antecedentes de los posibles empleados (dentro de los límites de las leyes locales) antes de contratar a los posibles empleados que tendrán acceso a los datos del titular de la tarjeta o al entorno de los datos del titular de la tarjeta.
12.8 Mantenga e implemente políticas y procedimientos para administrar los proveedores de servicios con quienes se compartirán datos del titular de la tarjeta, o que podrían afectar la seguridad de los datos del titular de la tarjeta de la siguiente manera: **12.8** A través de la observación, la revisión de políticas y procedimientos y el análisis de documentos de apoyo, verifique que se implementen los procesos para administrar a los proveedores de servicios con quienes se compartirán datos del titular de la tarjeta, o que podrían afectar la seguridad de los datos del titular de la tarjeta de la siguiente manera:
12.8.1 Mantener una lista de proveedores de servicios, incluida una descripción del servicio prestado. **12.8.1** Verifique que se mantiene una lista de proveedores de servicios y que incluya una descripción del servicio prestado.
12.8.2 Mantenga un acuerdo por escrito en el que los proveedores de servicios aceptan responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente. **12.8.2** Observe los acuerdos escritos y confirme que los proveedores de servicios aceptan responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente.
12.8.3 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios, que incluya una auditoría adecuada previa al compromiso. **12.8.3** Verifique que las políticas y los procedimientos estén documentados e implementados, que incluyan una auditoría adecuada previa al compromiso con cualquier proveedor de servicios.
12.8.4 Mantenga un programa para monitorear el estado de cumplimiento de las PCI DSS por parte del proveedor de servicios. **12.8.4** Verifique que la entidad tenga un programa para monitorear el estado de cumplimiento de las PCI DSS por parte del proveedor de servicios.
12.8.5 Conserve información sobre cuáles son los requisitos de las PCI DSS que administra cada proveedor de servicios y cuáles administra la entidad. **12.8.5** Verifique que la entidad conserve información sobre cuáles son los requisitos de las PCI DSS que administra cada proveedor de servicios y cuáles administra la entidad.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
12.9 Requisitos adicionales solo para los proveedores de servicios: Los proveedores de servicios aceptan, por escrito y ante los clientes, responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente. **12.9** Procedimientos de pruebas adicionales para los proveedores de servicios: Revise las políticas y los procedimientos del proveedor de servicio y observe las plantillas de los acuerdos escritos para verificar que el proveedor de servicios acepta, por escrito y ante el cliente, mantener los requisitos correspondientes de las PCI DSS en la medida en que el proveedor de servicios posea o, de otra manera, manipule, almacene, procese o transmita datos del titular de la tarjeta en nombre del cliente, o datos de autenticación confidenciales, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente.
12.10 Implemente un plan de respuesta ante incidentes. Prepárese para responder de inmediato ante un fallo en el sistema. **12.10** Revise el plan de respuesta ante incidentes y los procedimientos relacionados para verificar que la entidad está preparada para responder inmediatamente ante una falla del sistema mediante lo siguiente **12.10.1** Desarrolle el plan de respuesta ante incidentes que se implementará en caso de que ocurra una falla del sistema. Asegúrese de que el plan aborde, como mínimo, lo siguiente: · Roles, responsabilidades y estrategias de comunicación y contacto en caso de un riesgo que incluya, como mínimo, la notificación de las marcas de pago. · Procedimientos específicos de respuesta a incidentes. · Procedimientos de recuperación y continuidad comercial. · Procesos de copia de seguridad de datos. · Análisis de los requisitos legales para el informe de riesgos. · Cobertura y respuestas de todos los componentes críticos del sistema. · Referencia o inclusión de procedimientos de respuesta ante incidentes de las marcas de pago. **12.10.1.a** Verifique que el plan de respuesta ante incidentes incluya lo siguiente: · Las funciones, responsabilidades y estrategias de comunicación en caso de un riesgo que incluya como mínimo la notificación de las marcas de pago; · Procedimientos específicos de respuesta a incidentes. · Procedimientos de recuperación y continuidad comercial. · Procesos de copia de seguridad de datos. · Análisis de requisitos legales para el informe de riesgos (por ejemplo, la ley 1386 del Senado de California que exige la notificación de los consumidores afectados en caso de un riesgo real o supuesto por operaciones comerciales con residentes de California en su base de datos). · La cobertura y respuestas de todos los componentes críticos del sistema; · Referencia o inclusión de procedimientos de respuesta ante incidentes de las marcas de pago. **12.10.1.b** Entreviste al personal y revise la documentación de la muestra de un incidente o una alerta anteriormente informados para verificar que se hayan respetado los procedimientos y el plan de respuesta ante incidentes documentados.
12.10.2 Revise y pruebe el plan, incluidos todos los elementos enumerados en el Requisito 12.10.1, al menos anualmente. **12.10.2** Entreviste al personal y revise la documentación de las pruebas para verificar que el plan se prueba al menos anualmente, y que la prueba incluye todos los elementos enumerados en el Requisito 12.10.1.
12.10.3 Designe a personal específico para que esté disponible las 24 horas al día, los 7 días de la semana para responder a las alertas. **12.10.3** Mediante la observación, revise las políticas y entreviste al personal responsable para verificar que el personal designado esté siempre disponible (24 horas del día, los 7 días de la semana) para responder ante incidentes y que monitoreen la cobertura de cualquier evidencia de actividad no autorizada, detección de puntos de acceso inalámbricos no autorizados, alertas críticas de IDS (sistemas de intrusión-detección) o informes de cambios no autorizados en archivos de contenido o de sistemas críticos.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
12.10.4 Capacite adecuadamente al personal sobre las responsabilidades de respuesta ante fallas de seguridad. **12.10.4** Mediante la observación, la revisión de las políticas y las entrevistas al personal responsable verifique que el personal se capacite periódicamente en las responsabilidades ante fallas de seguridad.
12.10.5 Incluya alertas de los sistemas de supervisión de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, firewalls y sistemas de supervisión de integridad de archivos. **12.10.5** Mediante la observación y revisión de los procesos, verifique que, en el plan de respuesta ante incidentes, se incluya la supervisión y respuesta a las alertas de los sistemas de seguridad.
12.10.6 Elabore un proceso para modificar y desarrollar el plan de respuesta ante incidentes según las lecciones aprendidas e incorporar los desarrollos de la industria. **12.10.6** Mediante la observación, la revisión de las políticas y las entrevistas al personal responsable verifique que exista un proceso para modificar y desarrollar el plan de respuesta ante incidentes según las lecciones aprendidas e incorporar los desarrollos de la industria.
12.11.1 Requisitos adicionales solo para los proveedores de servicios: Mantener la documentación del proceso de revisión trimestral para incluir: · Documentar los resultados de las revisiones · Revisión y cierre de los resultados por el personal asignado a la responsabilidad del programa de cumplimiento de la PCI DSS **12.11.1** Revise la documentación de las revisiones trimestrales para verificar que incluyen: · Documentar los resultados de las revisiones · Revisión y cierre de los resultados por el personal asignado a la responsabilidad del programa de cumplimiento de la PCI DSS
A.1 Proteger el entorno y los datos alojados de cada entidad (es decir comerciante, proveedor de servicios u otra entidad), según los puntos A.1.1 a A.1.4: Un proveedor de hosting debe cumplir con estos requisitos, así como también con las demás secciones correspondientes de PCI DSS. Nota: Aunque posiblemente el proveedor de hosting cumpla con estos requisitos, no se garantiza el cumplimiento de la entidad que utiliza al proveedor de hosting. Cada entidad debe cumplir con las PCI DSS y validar el cumplimiento, según corresponda. A.1 En el caso específico de la evaluación de las PCI DSS de un proveedor de hosting compartido, verifique que los proveedores de hosting compartido protejan los datos y el entorno alojado de las entidades (comerciantes y proveedores de servicios), seleccione una muestra de servidores (Microsoft Windows y Unix/Linux) a través de una muestra representativa de comerciantes y proveedores de servicios alojados, y realice de los puntos de A.1.1 a A.1.4 a continuación:
A.1.1 Asegúrese de que cada entidad solo implemente procesos que tengan acceso al entorno de datos del titular de la tarjeta de la entidad. **A.1.1** Si un proveedor de hosting compartido permite a las entidades (por ejemplo, comerciantes o proveedores de servicios) ejecutar sus propias aplicaciones, verifique que estos procesos de aplicación se ejecuten utilizando la ID única de la entidad. Por ejemplo: • Ninguna entidad del sistema puede utilizar una ID de usuario de servidor Web compartida. • Todas las secuencias de comandos CGI utilizadas por una entidad se deben crear y ejecutar como ID de usuario única de la entidad.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
A.1.2 Limite el acceso y los privilegios de cada entidad solo al entorno de sus propios datos del titular de la tarjeta. **A.1.2.a** Verifique que la ID de usuario de cualquier proceso de aplicación no sea un usuario con privilegios (raíz/admin). **A.1.2.b** Verifique que cada entidad (comerciante, proveedor de servicios) haya leído, escrito o ejecute permisos sólo para los archivos y directorios que tiene o para los archivos necesarios para el sistema (restringidos mediante permisos de sistema de archivos, listas de control de acceso, chroot, jailshell, etc.) Importante: Los archivos de una entidad no deben compartirse de forma grupal. **A.1.2.c** Verifique que los usuarios de la entidad no tengan acceso de escritura a los archivos binarios compartidos del sistema. **A.1.2.d** Verifique que la visualización de las entradas del registro se restrinja a la entidad propietaria. **A.1.2.e** Para asegurarse de que ninguna entidad monopoliza los recursos del servidor y se aproveche de las vulnerabilidades (por ejemplo, error, carrera y condiciones de reinicio que tienen como consecuencia, por ejemplo, desbordamientos de buffer), verifique que se apliquen las restricciones para el uso de estos recursos del sistema: • Espacio en disco • Ancho de banda • Memoria CPU
A.1.3 Asegúrese de que los registros y las pistas de auditoría estén habilitados y sean exclusivos para el entorno de datos del titular de la tarjeta de cada entidad y que cumplan con el Requisito 10 de las PCI DSS. **A1.3** Verifique que el proveedor de hosting compartido haya habilitado los registros de la siguiente manera para cada comerciante y entorno de proveedor de servicios: · Los registros se habilitan para aplicaciones comunes de terceros. · Los registros están activos de forma predeterminada. · Los registros están disponibles para la revisión de la entidad propietaria. · La ubicación de los registros se comunica con claridad a la entidad propietaria.
A1.4 Habilite los procesos para que se realice una investigación forense oportuna en caso de que un comerciante o proveedor de servicios alojado corra riesgos. **A1.4** Verifique que el proveedor de hosting compartido cuente con políticas escritas que especifiquen la realización de una investigación forense oportuna de los servidores relacionados en caso de riesgo.
A2.1 Donde las terminales POS POI (y los puntos de terminación de SSL/TLS a los que se conectan) utilizan SSL y/o TLS temprana, la entidad debe: · Confirmar que los dispositivos no son susceptibles a los ataques conocidos para aquellos protocolos. ***O:*** · Tener un Plan de migración y de mitigación de riesgo formal implementado. **A2.1** *Para las terminales POS POI (los puntos de terminación de SSL/TLS para los que se conectan) el uso de SSL y/o TLS temprana:* · Confirmar que la entidad cuenta con la documentación (por ejemplo, documentación del proveedor, detalles de configuración de la red/sistema, etc.) que verifica que los dispositivos no son susceptibles a los ataques conocidos para SSL/TLS temprana. *O:* · Complete A2.2 a continuación.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
A2.2 Las entidades con las implementaciones existentes (excepto según lo permitido en A2.1) que utilizan SSL y/o TLS temprana deben tener un Plan de Migración y de mitigación del riesgo implementados. **A2.2** Revise el Plan de Migración y de mitigación del riesgo documentado para verificar que incluya: · Descripción del uso, incluidos los datos que se están transmitiendo, los tipos y el número de sistemas que utilizan y/o dan soporte a SSL/TLS temprana, el tipo de entorno; · Resultados de la evaluación de riesgos y controles de reducción de riesgos implementados; · Descripción de los procesos a monitorear para las nuevas vulnerabilidades asociadas con SSL/TLS temprana; · Descripción de los procesos de control de cambios que se implementan para garantizar que SSL/TLS temprana no se implementa en los nuevos entornos; · Descripción general del plan de proyecto de migración que incluye la fecha de finalización de la migración objetivo no más tarde del 30 de junio de 2018.
A2.3 ***Requisitos adicionales solo para los proveedores de servicios:*** Todos los proveedores de servicios deben ofrecer una oferta de servicios segura al 30 de junio de 2016. ***Nota:*** *Con anterioridad al 30 de junio de 2016, el proveedor de servicios debe tener una opción de protocolo seguro incluida en su oferta de servicios,* ***o*** *tener un Plan de migración y mitigación de riesgos documentado (según A2.2) que incluya una fecha límite para la provisión de una opción de protocolo seguro no más tarde del 30 de junio de 2016.* *Después de esta fecha, todos los proveedores de servicios deben ofrecer una opción de protocolo seguro para su servicio.* **A2.3** Revise las configuraciones del sistema y la documentación de apoyo para verificar que el proveedor de servicios ofrece una opción de protocolo seguro para su servicio.
A3.1.1 La gerencia ejecutiva deberá establecerá la responsabilidad de la protección de los datos del titular de la tarjeta y un programa de cumplimiento de la PCI DSS para incluir: • Responsabilidad general de mantener el cumplimiento de la PCI DSS • La definición de un estatuto para el programa de cumplimiento de la PCI DSS • Proporcionar actualizaciones a la gerencia ejecutiva y a la junta directiva sobre las iniciativas y los problemas de cumplimiento de la PCI DSS, incluidas las actividades de remediación, al menos anualmente Referencia de la PCI DSS: Requisito 12 **A3.1. 1.a** Revise la documentación para verificar que la gerencia ejecutiva ha asignado la responsabilidad general de mantener el cumplimiento de la PCI DSS de la entidad. **A3.1.1. b** Revise el estatuto de la PCI DSS de la empresa para verificar que se describen las condiciones en las que se organiza el programa de cumplimiento de la PCI DSS. **A3.1.1.c** Revise las actas de reuniones y/o presentaciones de la gerencia ejecutiva y la junta directiva para garantizar que las iniciativas de cumplimiento de la PCI DSS y las actividades de remediación se comunican al menos anualmente.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
A3.1.2 Un programa formal de cumplimiento de la PCI DSS debe estar implementado para incluir: • Definición de las actividades para mantener y supervisar el cumplimiento general de la PCI DSS, incluidas las actividades habituales • Procesos anuales de evaluación de la PCI DSS • Los procesos para la validación continua de los requisitos de la PCI DSS (por ejemplo: diarios, semanales, trimestrales, etc. según sea aplicable de acuerdo al requisito) • Un proceso para realizar el análisis del impacto comercial para determinar los posibles impactos de la PCI DSS para las decisiones estratégicas comerciales ***Referencia de la PCI DSS:*** *Requisitos 1-12* **A3.1. 2.a** Revise las políticas y los procedimientos de seguridad de la información para verificar que los procesos estén definidos para realizar lo siguiente: • Mantener y supervisar el cumplimiento general de la PCI DSS, incluidas las actividades habituales • Evaluaciones anuales de la PCI DSS • Validación continua de los requisitos de la PCI DSS • Análisis del impacto comercial para determinar los posibles impactos de la PCI DSS para las decisiones comerciales estratégicas **A3.1.2. b** Entreviste al personal y observe las actividades de cumplimiento para verificar que los procesos definidos son implementados para lo siguiente: • Mantener y supervisar el cumplimiento general de la PCI DSS, incluidas las actividades habituales • Evaluaciones anuales de la PCI DSS • Validación continua de los requisitos de la PCI DSS • Análisis del impacto comercial para determinar los posibles impactos de la PCI DSS para las decisiones comerciales estratégicas
A3.1.3 Los roles y las responsabilidades de cumplimiento de la PCI DSS deben definirse específicamente y asignarse formalmente a uno o más miembros del personal, incluido al menos lo siguiente: • Gestionar las actividades habituales de la PCI DSS • Gestionar las evaluaciones anuales de la PCI DSS • Gestionar la validación continua de los requisitos de la PCI DSS (por ejemplo: diarios, semanales, trimestrales, etc. según sea aplicable de acuerdo con el requisito) • Gestionar el análisis del impacto comercial para determinar los posibles impactos de la PCI DSS para las decisiones comerciales estratégicas Referencia de la PCI DSS: Requisito 12 **A3.1. 3.a** Revise las políticas y procedimientos de la seguridad de la información y entreviste al personal para verificar que los roles y las responsabilidades están claramente definidos y que las tareas se asignan para incluir al menos lo siguiente: • Gestionar las actividades habituales de la PCI DSS • Gestionar las evaluaciones anuales de la PCI DSS • Gestionar la validación continua de los requisitos de la PCI DSS (por ejemplo: diarios, semanales, trimestrales, etc. según sea aplicable de acuerdo con el requisito) • Gestionar el análisis del impacto comercial para determinar los posibles impactos de la PCI DSS para las decisiones comerciales estratégicas **A3.1.3. b** Entreviste al personal responsable y verifique que estén familiarizados con el desempeño designado de sus responsabilidades y de cumplimiento de la PCI DSS

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
A3.1.4 Proporcione capacitación sobre la seguridad de la información y/o la PCI DSS actualizada al menos anualmente para el personal con responsabilidades de cumplimiento de la PCI DSS (como se identifica en A3.1.3). Referencia de la PCI DSS: Requisito 12 **A3.1. 4.a** Revise las políticas y procedimientos de seguridad de la información para verificar que la capacitación sobre la seguridad de la información y/o la PCI DSS se requiere por lo menos anualmente para cada rol con las responsabilidades de cumplimiento de la PCI DSS. **A3.1.4. b** Entreviste al personal y revise los certificados de asistencia u otros registros para verificar que el personal con responsabilidad de cumplimiento de la PCI DSS recibe capacitación de seguridad de la información similar y/o de la PCI DSS actualizada al menos anualmente.
A3.2.1 Documentar y confirmar la precisión del alcance de la PCI DSS al menos trimestralmente y tras cambios significativos en el entorno del estudio. Como mínimo, la validación trimestral de alcance deberá incluir: • Identificar todas las redes en el alcance y los componentes del sistema • Identificar todas las redes en el alcance y la justificación para las redes que están fuera del alcance, incluidas las descripciones de todos los controles de segmentación implementados • La identificación de todas las entidades conectadas, por ejemplo, las entidades de terceros relacionadas con el acceso al entorno de los datos del titular de la tarjeta (CDE) Referencia de la PCI DSS: Alcance de los requisitos de la PCI DSS" **A3.2. 1a** Revise los resultados documentados de las revisiones del alcance y entreviste al personal para verificar que se realizan las revisiones: • Al menos trimestralmente • Después de cualquier cambio significativo en el entorno **A3.2.1. b** Revise los resultados documentados de las revisiones de alcance trimestralmente para verificar que se realiza lo siguiente: • Identificación de todas las redes en el alcance y los componentes del sistema • Identificación de todas las redes fuera del alcance y la justificación de las redes por estar fuera del alcance, incluidas las descripciones de todos los controles de segmentación implementados • Identificación de todas las entidades conectadas, por ejemplo, entidades de terceros con acceso al CDE
A3.2.2 Determine el impacto del alcance de la PCI DSS para todos los cambios en los sistemas o redes, incluidas las adiciones de nuevos sistemas y nuevas conexiones de red. Los procesos deben incluir: • La realización de una evaluación formal de impacto de la PCI DSS • La identificación de los requisitos de la PCI DSS aplicables al sistema o red • Actualización del alcance de la PCI DSS en su caso • Cierre documentado de los resultados de la evaluación de impacto por parte del personal responsable (como se define en A3.1.3) ***Referencia de la PCI DSS:*** *Alcance de los requisitos de la PCI DSS; Requisitos 1-12* **A3.2.2** Revise la documentación de cambio y entreviste al personal para verificarlo para cada cambio en los sistemas o redes: • Se realizó una evaluación formal del impacto de la PCI DSS. • Se identificaron los requisitos de la PCI DSS aplicables a los cambios en la red o en los sistemas. • Se actualiza el alcance de la PCI DSS según sea apropiado para el cambio. • Se obtuvo y documentó el cierre por parte del personal responsable (como se define en A3.1.3).

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
A3.2.2.1 Al término de un cambio, se deben verificar todos los requisitos de la PCI DSS pertinente en todos los sistemas y redes nuevos o modificados y se debe actualizar la documentación, según sea el caso. Ejemplos de requisitos de la PCI DSS que deben ser verificados incluyen, pero no se limitan a: ▪ El Diagrama de una red se actualiza para reflejar los cambios. ▪ Los sistemas están configurados según las normas de configuración, con todas las contraseñas predeterminadas cambiadas y los servicios innecesarios deshabilitados. ▪ Los sistemas están protegidos con los controles requeridos, por ejemplo, la supervisión de la integridad de archivos (FIM), los antivirus, los parches, y el registro de auditoría. ▪ Verifique que los datos confidenciales de autenticación (SAD) no se almacenan y que el almacenamiento de todos los datos del titular de la tarjeta (CHD) se documenta e incorpora en la política y los procedimientos de retención de datos ▪ Los nuevos sistemas se incluyen en el proceso trimestral de análisis de vulnerabilidad. ***Referencia de la PCI DSS:*** *Alcance de los requisitos de la PCI DSS; Requisito 1-12* **A3.2.2.1** Para una muestra de los cambios en los sistemas y en la red, revise los registros de cambios, entreviste al personal y observe los sistemas/redes afectados para verificar que se implementaron los requisitos aplicables de la PCI DSS y que se actualizó la documentación como parte del cambio.
A3.2.3 Los cambios en la estructura organizativa, por ejemplo, la fusión o la adquisición de empresas, el cambio o reasignación del personal encargado de los controles de seguridad, da lugar a una revisión formal (interna) del impacto del alcance de la PCI DSS y la aplicabilidad de los controles. ***Referencia de la PCI DSS:*** *Requisito 12* **A3.2.3** Examinar las políticas y procedimientos para verificar que un cambio en la estructura organizativa da lugar a la revisión formal del impacto del alcance de la PCI DSS y la aplicabilidad de los controles.
A3.2.4 Si se utiliza la segmentación, confirme el alcance de la PCI DSS al realizar pruebas de penetración en los controles de segmentación, al menos cada seis meses y después de cualquier cambio a los controles/métodos de segmentación. ***Referencia de la PCI DSS:*** *Requisito 11* **A3.2.4** Examinar los resultados de la prueba de penetración más reciente para verificar que: • La prueba de penetración se realiza para verificar los controles de segmentación, por lo menos cada seis meses y después de cualquier cambio a los controles/métodos de segmentación. • La prueba de penetración abarca todos los controles o métodos de segmentación implementados. • La prueba de penetración verifica que los métodos de segmentación sean operativos y eficaces, y que aíslan todos los sistemas fuera de alcance de los sistemas dentro del CDE.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
A3.2.5 Implemente una metodología de descubrimiento de datos para confirmar el alcance de la PCI DSS y para localizar todas las fuentes y ubicaciones de PAN en texto claro al menos trimestralmente y tras cambios significativos en el entorno o en los procesos del titular de tarjeta. La metodología de descubrimiento de datos debe tomar en consideración el potencial del PAN en texto claro para residir en los sistemas y en las redes fuera del CDE actualmente definido. Referencia de la PCI DSS: Alcance de los requisitos de la PCI DSS **A3.2. 5.a** Revise la metodología de descubrimiento de datos documentada para verificar lo siguiente: • La metodología de descubrimiento de datos incluye procesos para identificar todas las fuentes y ubicaciones del PAN en texto claro. • La metodología toma en consideración el potencial del PAN en texto claro para residir en los sistemas y en las redes fuera del CDE actualmente definido. **A3.2.5. b** Revise los resultados de los recientes esfuerzos de descubrimiento de datos, y entreviste al personal responsable para verificar que el descubrimiento de datos se lleva a cabo por lo menos trimestralmente y tras cambios significativos en el entorno o en los procesos del titular de tarjeta.
A3.2.5.1 Garantice la eficacia de los métodos utilizados para el descubrimiento de los datos—por ejemplo, los métodos deben ser capaces de descubrir el PAN en texto claro en todos los tipos de componentes del sistema (por ejemplo, en cada sistema operativo o plataforma) y formatos de archivo en uso. Se debe confirmar la eficacia de los métodos de descubrimiento de datos por lo menos anualmente. Referencia de la PCI DSS: Alcance de los requisitos de la PCI DSS **A3.2.5. 1.a** Entreviste al personal y revise la documentación para verificar que: ▪ La entidad tiene un proceso implementado para probar la eficacia de los métodos utilizados para el descubrimiento de datos. ▪ El proceso incluye la verificación de los métodos que son capaces de descubrir el PAN en texto claro sobre todos los tipos de componentes del sistema y los formatos de archivo en uso. **A3.2.5.1. b** Revise los resultados de las pruebas de efectividad recientes para verificar que se confirma la eficacia de los métodos utilizados para el descubrimiento de datos, por lo menos anualmente.
A3.2.5.2 Implemente procedimientos de respuesta a iniciar tras la detección del PAN en texto claro fuera del CDE para incluir: ▪ Procedimientos para determinar qué hacer si el PAN en texto claro se descubre fuera del CDE, incluidas su recuperación, eliminación segura y/o migración en el CDE definido actualmente, según sea el caso ▪ Procedimientos para determinar cómo los datos terminaron fuera del CDE ▪ Procedimientos para remediar las fugas de datos o las brechas de procesos que dieron lugar a que los datos queden fuera del CDE ▪ Procedimientos para identificar la fuente de los datos ▪ Procedimientos para identificar si datos de la pista se almacenan con el PAN

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
A3.2.5.2.a Revise los procedimientos de respuesta documentados para verificar que se definen e incluyen los procedimientos para responder a la detección del PAN en texto claro fuera del CDE: ▪ Procedimientos para determinar qué hacer si el PAN en texto claro se descubre fuera del CDE, incluidas su recuperación, eliminación segura y/o migración en el CDE definido actualmente, según sea el caso ▪ Procedimientos para determinar cómo los datos terminaron fuera del CDE ▪ Procedimientos para remediar las fugas de datos o las brechas de procesos que dieron lugar a que los datos queden fuera del CDE ▪ Procedimientos para identificar la fuente de los datos ▪ Procedimientos para identificar si datos de la pista se almacenan con el PAN **A3.2.5.2. b** Entreviste al personal y examine los registros de las medidas de respuesta para que las actividades de remediación se realicen cuando se detecta el PAN en texto claro fuera del CDE.
A3.2.6 Implemente mecanismos para detectar y prevenir que el PAN en texto claro salga del CDE a través de un canal, método o proceso no autorizado, incluida la generación de registros de auditoría y alertas. Referencia de la PCI DSS: Alcance de los requisitos de la PCI DSS **A3.2. 6.a** Revise la documentación y observe los mecanismos implementados para verificar que los mecanismos están: • Implementados y funcionando activamente • Configurados para detectar y prevenir que el PAN en texto claro sale del CDE a través de un canal, método o proceso no autorizado • Generando registros y alertas tras la detección del PAN en texto claro que sale del CDE a través de un canal, método o proceso no autorizado **A3.2.6. b** Revise los registros de auditoría y las alertas, y entreviste al personal responsable para verificar que las alertas se investigan.
A3.2.6.1 Implemente los procedimientos de respuesta a iniciar tras la detección de intentos de eliminar el PAN en texto claro del CDE a través de un canal, método o proceso no autorizado. Los procedimientos de respuesta deben incluir: • Procedimientos para la investigación oportuna de alertas por parte del personal responsable • Procedimientos para remediar las fugas de datos o las brechas del proceso, según sea necesario, para evitar cualquier pérdida de datos **A3.2.6. 1.a** Revise los procedimientos documentados de respuesta para verificar que los procedimientos para responder al intento de eliminación del PAN en texto claro del CDE a través de un canal, método o proceso no autorizado incluyen: • Procedimientos para la investigación oportuna de alertas por parte del personal responsable • Procedimientos para remediar las fugas de datos o las brechas del proceso, según sea necesario, para evitar cualquier pérdida de datos **A3.2.6.1. b** Entreviste al personal y revise los registros de las medidas tomadas cuando se detecta que el PAN en texto claro sale del CDE a través de un canal, método o proceso no autorizado y verifique que se realizaron las actividades de remediación.

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
A3.3.1 Implemente un proceso para detectar y alertar de inmediato las fallas de control de seguridad críticas. Ejemplos de controles de seguridad críticos incluyen, pero no se limitan a: • Firewalls • IDS/IPS • FIM • Antivirus • Controles de acceso físicos • Controles de acceso lógico • Mecanismos de registro de auditoría • Controles de segmentación (si se utilizan) Referencia de la PCI DSS: Requisitos 1-12 **A3.3. 1.a** Revise las políticas y los procedimientos documentados para verificar que los procesos están definidos para detectar y alertar de inmediato sobre las fallas críticas de control de seguridad. **A3.3.1. b** Revise los procesos de detección y de alerta y entreviste al personal para verificar que los procesos se implementan para todos los controles de seguridad críticos, y que la falla de un control de seguridad crítico da lugar a la generación de una alerta.
A3.3.1.1 Responda a las fallas de los controles de seguridad críticos de manera oportuna. Los procesos para responder en caso de fallas en el control de seguridad son los siguientes: • Restaurar las funciones de seguridad • Identificar y documentar la duración (fecha y hora de inicio a fin) de la falla de seguridad • Identificar y documentar las causas de la falla, incluida la causa raíz, y documentar la remediación requerida para abordar la causa raíz • Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad • Realizar una evaluación de riesgos para determinar si se requieren más acciones como resultado de la falla de seguridad • Implementar controles para prevenir que se vuelva a producir la causa de la falla • Reanudar la supervisión de los controles de seguridad Referencia de la PCI DSS: Requisitos 1-12 **A3.3.1.1.a** Revise las políticas y los procedimientos documentados y entreviste al personal para verificar que los procesos se definen e implementan para responder a una falla en el control de seguridad, e incluya: ▪ Restaurar las funciones de seguridad ▪ Identificar y documentar la duración (fecha y hora de inicio a fin) de la falla de seguridad ▪ Identificar y documentar las causas de la falla, incluida la causa raíz, y documentar la remediación requerida para abordar la causa raíz ▪ Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad ▪ Realizar una evaluación de riesgos para determinar si se requieren más acciones como resultado de la falla de seguridad ▪ Implementar controles para prevenir que se vuelva a producir la causa de la falla ▪ Reanudar la supervisión de los controles de seguridad **A3.3.1.1. b** Revise los registros para verificar que se documentan las fallas de control de seguridad para incluir: ▪ Identificación de las causas de la falla, incluida la causa raíz ▪ Duración (fecha y hora de inicio y fin) de la falla de seguridad ▪ Detalles de la remediación necesaria para abordar la causa raíz

Fuente: (PCI Security Standards Council, 2016)

Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
A3.3.2 Revise las tecnologías de hardware y software por lo menos anualmente para confirmar si siguen cumpliendo los requisitos de la PCI DSS de la organización. (Por ejemplo, una revisión de las tecnologías que ya no reciben soporte del proveedor y y/o que ya no cumplen con las necesidades de seguridad de la organización.) El proceso incluye un plan para remediar las tecnologías que ya no cumplen con los requisitos de la PCI DSS de la organización, hasta e incluido el reemplazo de la tecnología, según sea el caso. Referencia de la PCI DSS: Requisitos 2, 6 **A3.3. 2.a** Revise las políticas y los procedimientos documentados y entreviste al personal para verificar que los procesos se definen e implementan para revisar las tecnologías de hardware y software y confirmar si siguen cumpliendo con los requisitos de la PCI DSS de la organización. **A3.3.2. b** Revise los resultados de las recientes revisiones para verificar que las revisiones se realizan por lo menos anualmente. **A3.3.2.c** Para cualquier tecnología que se ha determinado que ya no cumple con los requisitos de la PCI DSS de la organización, verifique que un plan está implementado para remediar la tecnología.
A3.3.3 Realizar revisiones por lo menos trimestralmente para verificar que se siguen las actividades de BAU. Las revisiones deben ser realizadas por el personal asignado al programa de cumplimiento de la PCI DSS (como se identifica en A3.1.3), e incluyen lo siguiente: • Confirmación de que se realizan todas las actividades de BAU (por ejemplo, A3.2.2, A3.2.6 y A3.3.1) • Confirmación de que el personal sigue las políticas de seguridad y los procedimientos operativos (por ejemplo, las revisiones del registro diario, las revisiones del conjunto de reglas de firewall, las normas de configuración para nuevos sistemas, etc.) • Documentar cómo se completaron las revisiones, incluido cómo se verificaron todas las actividades BAU como implementadas. • Se requiere la recopilación de la evidencia documentada para la evaluación anual de la PCI DSS • Revisión y cierre de los resultados por el personal asignado con la responsabilidad del programa de cumplimiento de la PCI DSS (como se identifica en A3.1.3) • Retención de registros y la documentación durante al menos 12 meses, que abarcan todas las actividades BAU Referencia de la PCI DSS: Requisitos 1-12 **A3.3. 3.a** Revise las políticas y los procedimientos para verificar que los procesos se definen para la revisión y verificación de las actividades BAU. Verifique que los procesos incluyan: • Confirmar que todas las actividades BAU (por ejemplo, A3.2.2, A3.2.6 y A3.3.1) se realizan • Confirmar que el personal siga las políticas de seguridad y los procedimientos operativos (por ejemplo, las revisiones del registro diario, las revisiones del conjunto de reglas de firewall, las normas de configuración para nuevos sistemas, etc.) • Documentar cómo se completaron las revisiones, incluido cómo se verificaron todas las actividades BAU como implementadas • Recopilar la evidencia documentada según se requiera para la evaluación anual de la PCI DSS • La revisión y cierre de los resultados por parte de la gerencia ejecutiva con la responsabilidad asignada del gobierno de la PCI DSS • Mantener los registros y la documentación durante al menos 12 meses, que cubra todas las actividades BAU

Fuente: (PCI Security Standards Council, 2016)

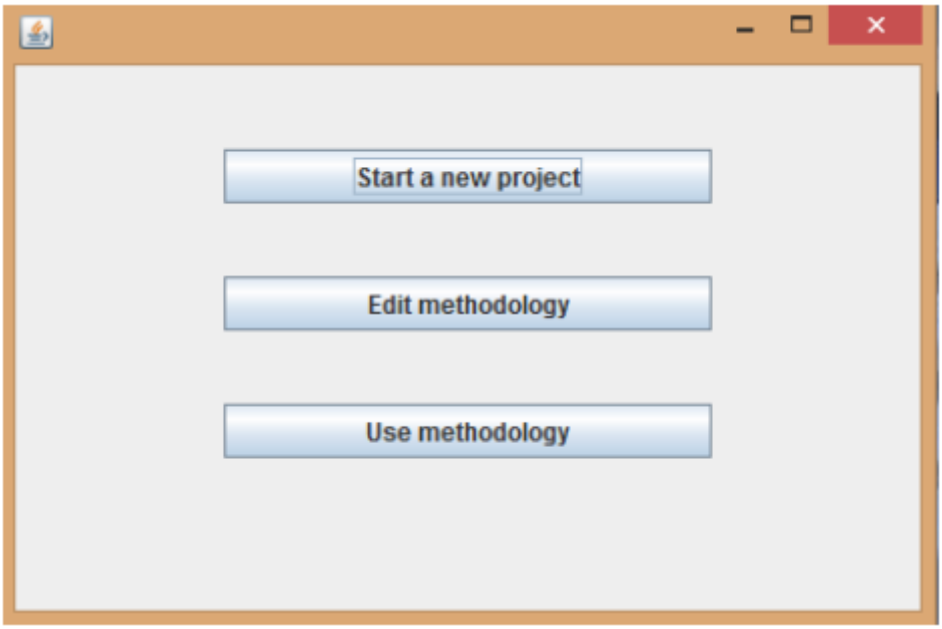
Tabla 27 - Requisitos y controles de seguridad de la información PCI-DSS v3.2 (Continuación)

Requisitos de las PCI DSS
A3.3.3. b Entreviste al personal responsable y examine los registros de las revisiones para verificar que: • Las revisiones las realiza el personal asignado al programa de cumplimiento de la PCI DSS • Las revisiones se realizan por lo menos trimestralmente
A3.4.1 Revise las cuentas de usuario y los privilegios de acceso a los componentes del sistema en el alcance por lo menos cada seis meses para garantizar que las cuentas y el acceso de usuario siguen siendo adecuados en función al trabajo, y a lo autorizado. ***Referencia de la PCI DSS:*** *Requisito 7* **A3.4.1** Entreviste al personal y revise la documentación de respaldo para verificar lo siguiente: • Las cuentas de usuario y los privilegios de acceso se revisan por lo menos cada seis meses. • Las revisiones confirman que el acceso es adecuado en función al trabajo, y que todo acceso está autorizado.
A3.5.1 Implementar una metodología para la identificación oportuna de los patrones de ataque y el comportamiento no deseado en todos los sistemas, por ejemplo, utilizar revisiones manuales coordinadas y/o herramientas de correlación de registro automatizadas que incluyan al menos lo siguiente: • Identificación de anomalías o actividades sospechosas, a medida que se producen • La emisión de alertas oportunas tras la detección de actividades sospechosas o anomalías para el personal responsable • Respuesta a las alertas de acuerdo con los procedimientos documentados de respuesta Referencia de la PCI DSS: Requisitos 10, 12 **A3.5.1.a** Revise la documentación y entreviste al personal para verificar que se define y se implementa una metodología para identificar los patrones de ataque y un comportamiento no deseado en todos los sistemas de manera oportuna, y que incluya lo siguiente: • Identificación de anomalías o actividades sospechosas, a medida que se producen • Emisión de alertas oportunas para el personal responsable • Respuesta a las alertas de acuerdo con los procedimientos documentados de respuesta **A3.5.1. b** Revise los procedimientos de respuesta a incidentes y entreviste al personal responsable para verificar que: • El personal de turno recibe alertas oportunas. • Se responde a las alertas según los procedimientos de respuesta documentados.

Fuente: (PCI Security Standards Council, 2016)

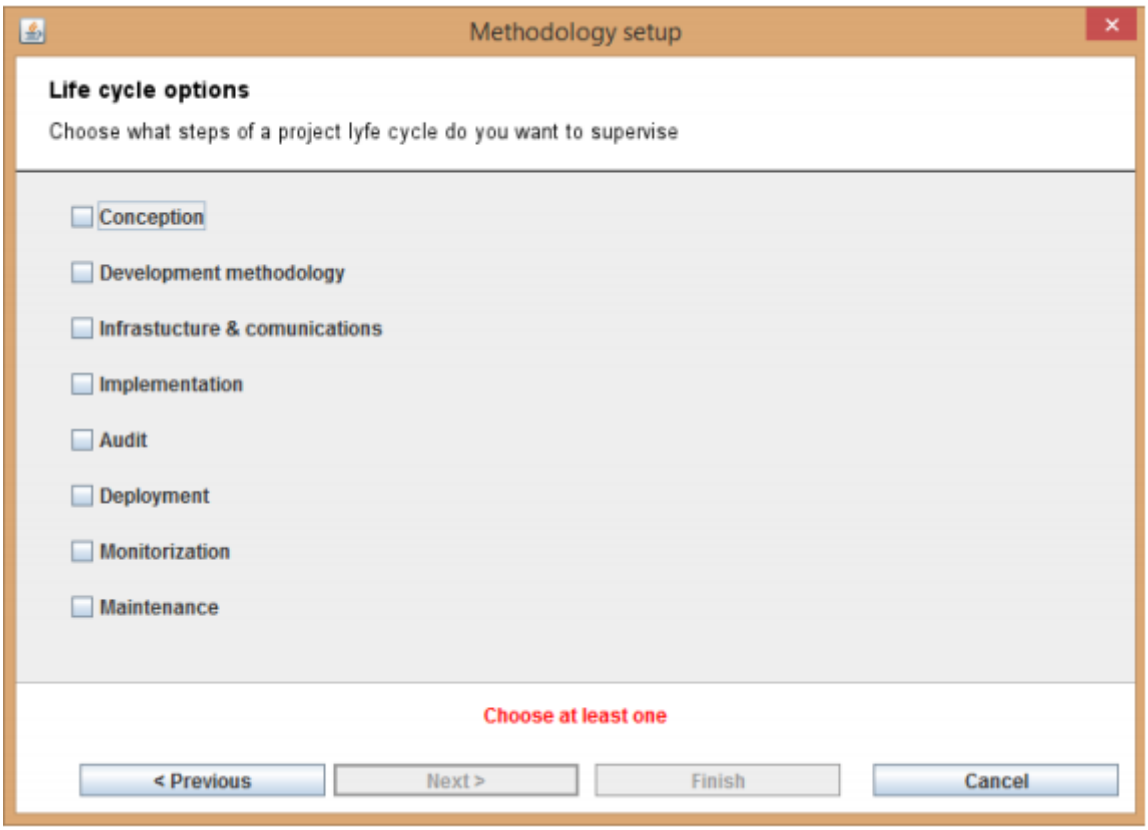
A5. Interfaz plataforma S2D2

Figura 40 – Interfaz Proyecto S2D2



Fuente: (Lopez Provencio, 2015)

Figura 40 – Interfaz S2D2(continuación)



Fuente: (Lopez Provencio, 2015)

Figura 40 – Interfaz S2D2(continuación)

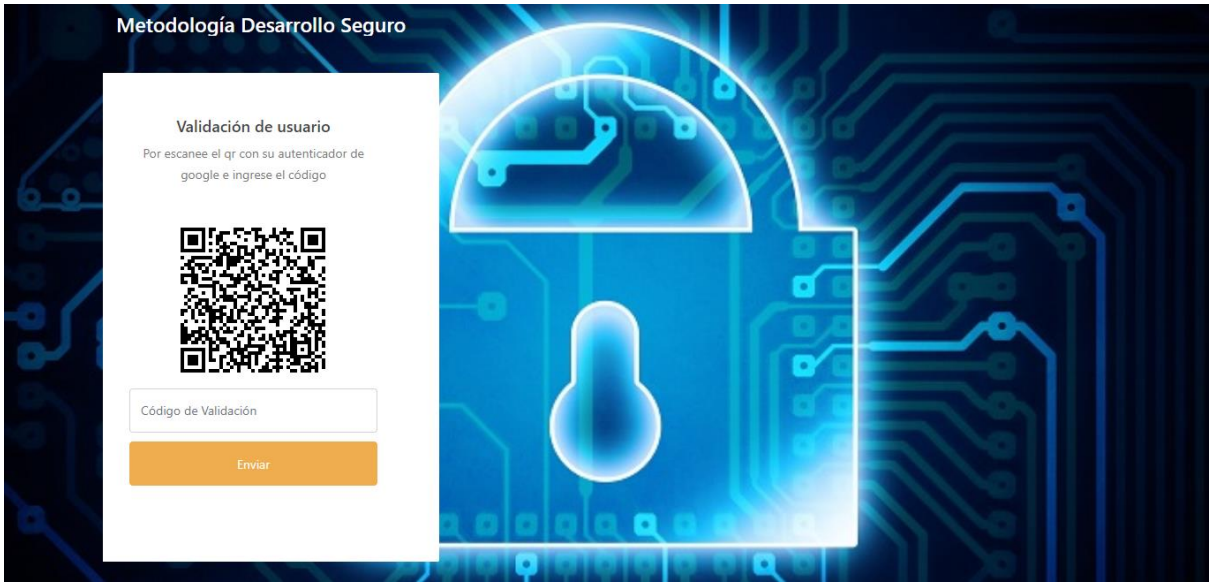
Fuente: (Lopez Provencio, 2015)

A.6 Plataforma Web

Figura 41 – Visualización página web

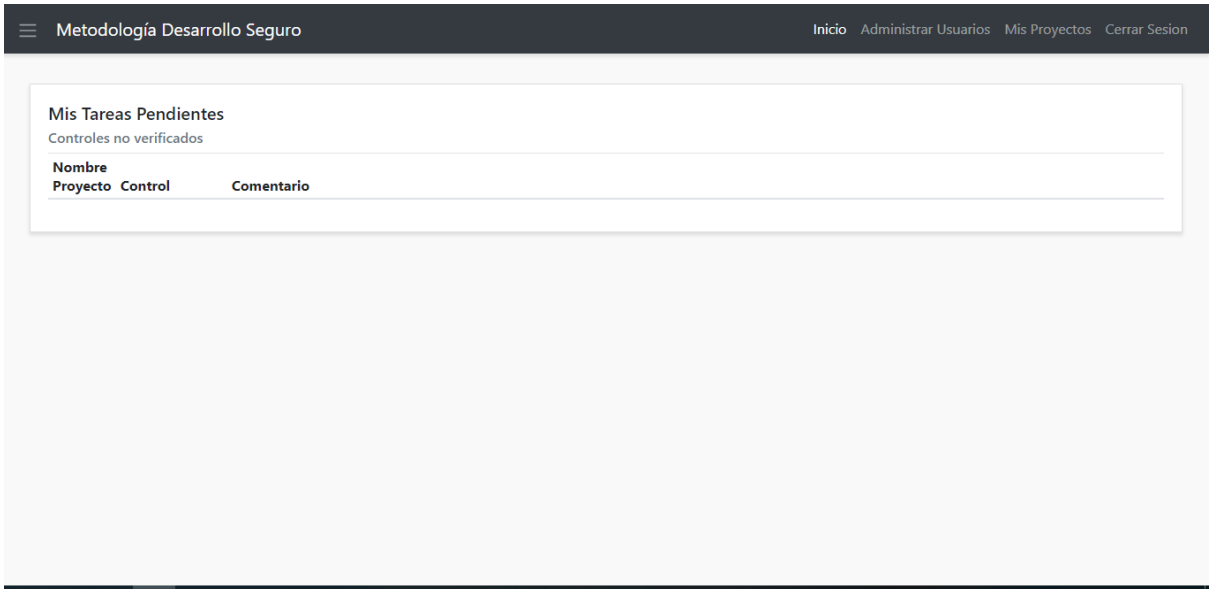
Fuente: Elaboración Propia

Figura 41 – Visualización página web(continuación)



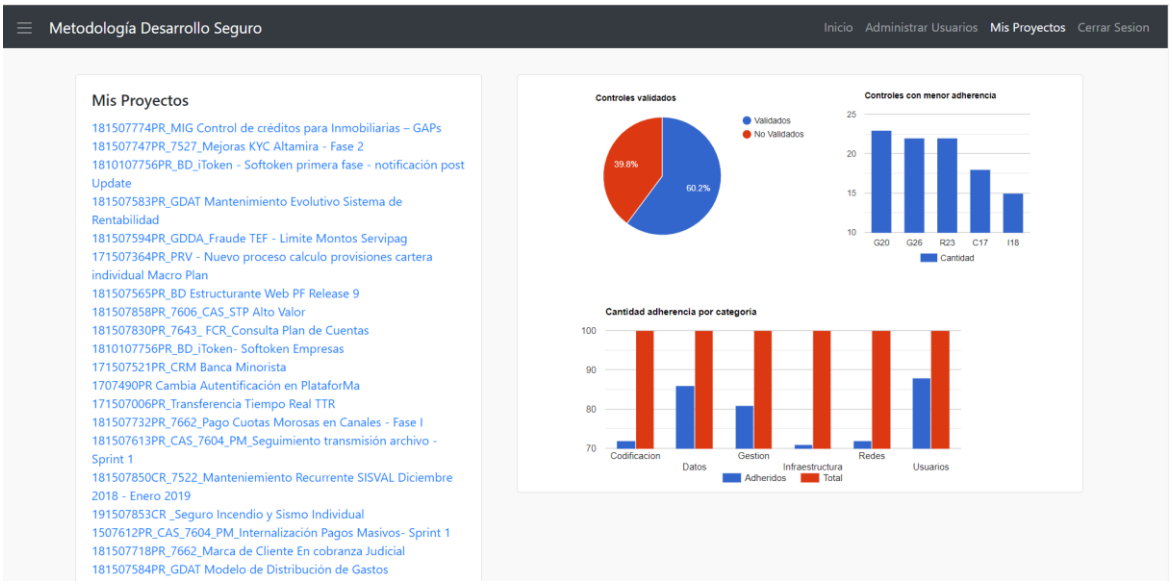
Fuente: Elaboración Propia

Figura 41 – Visualización página web(continuación)



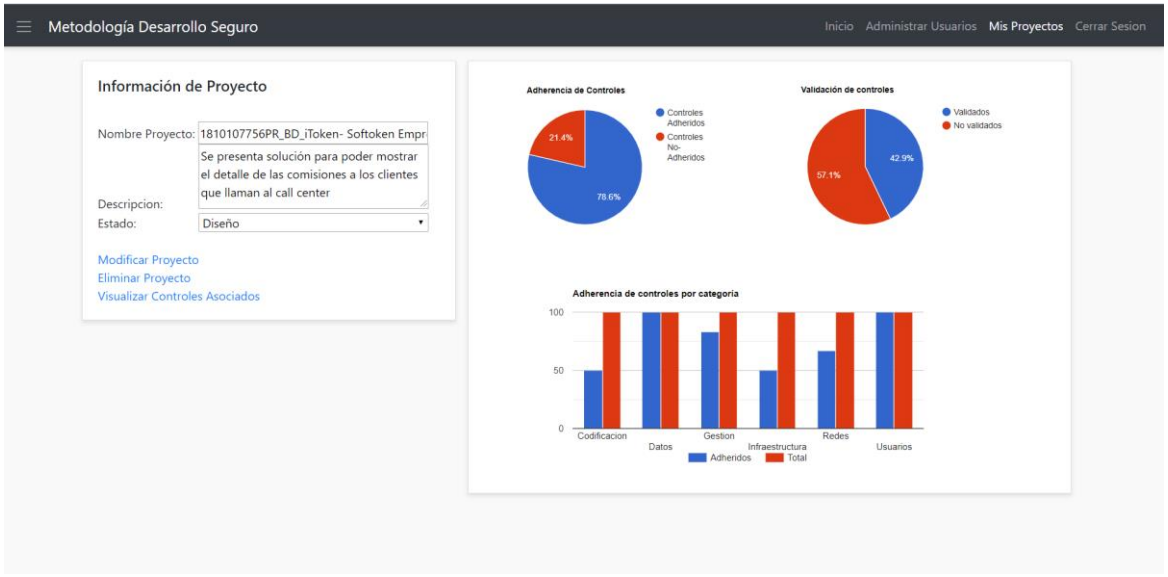
Fuente: Elaboración Propia

Figura 41 – Visualización página web(continuación)



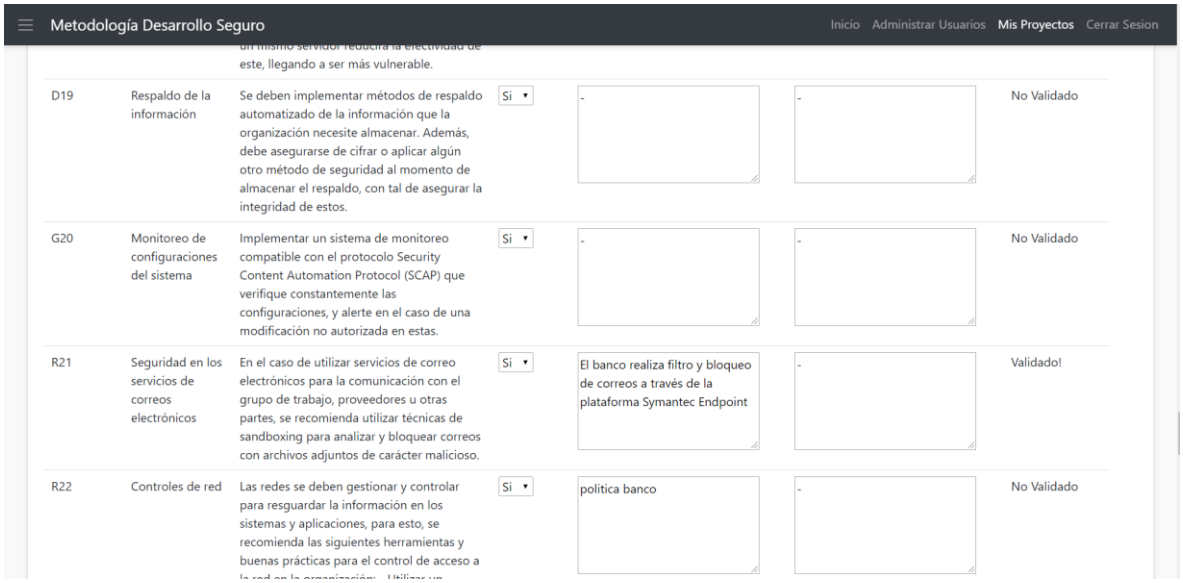
Fuente: Elaboración Propia

Figura 41 – Visualización página web(continuación)



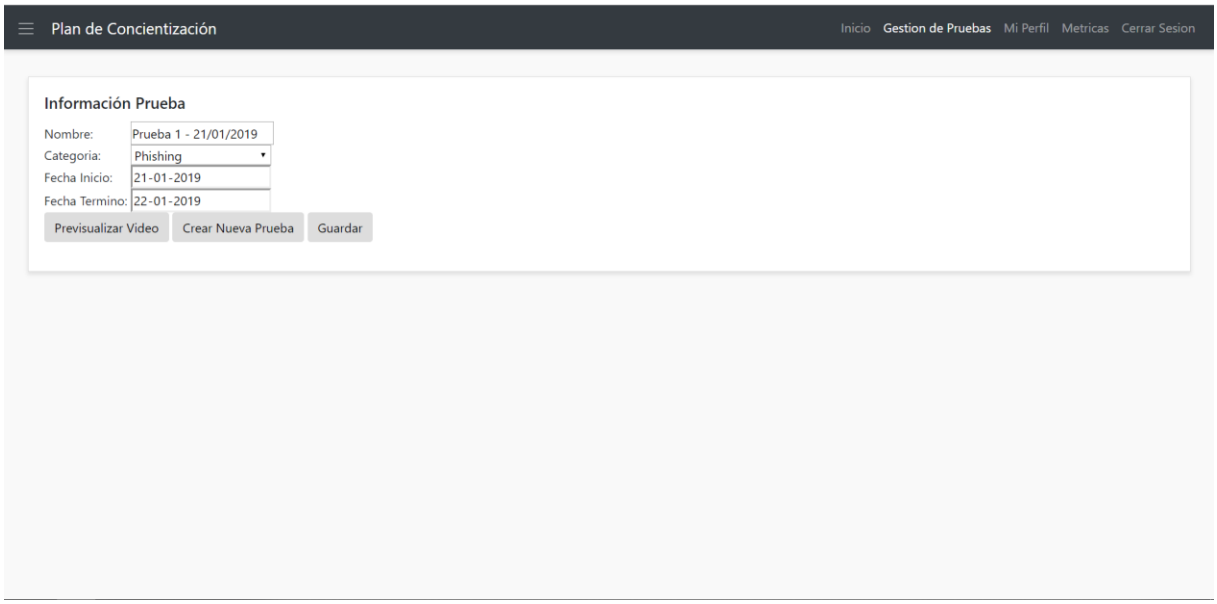
Fuente: Elaboración Propia

Figura 41 – Visualización página web(continuación)



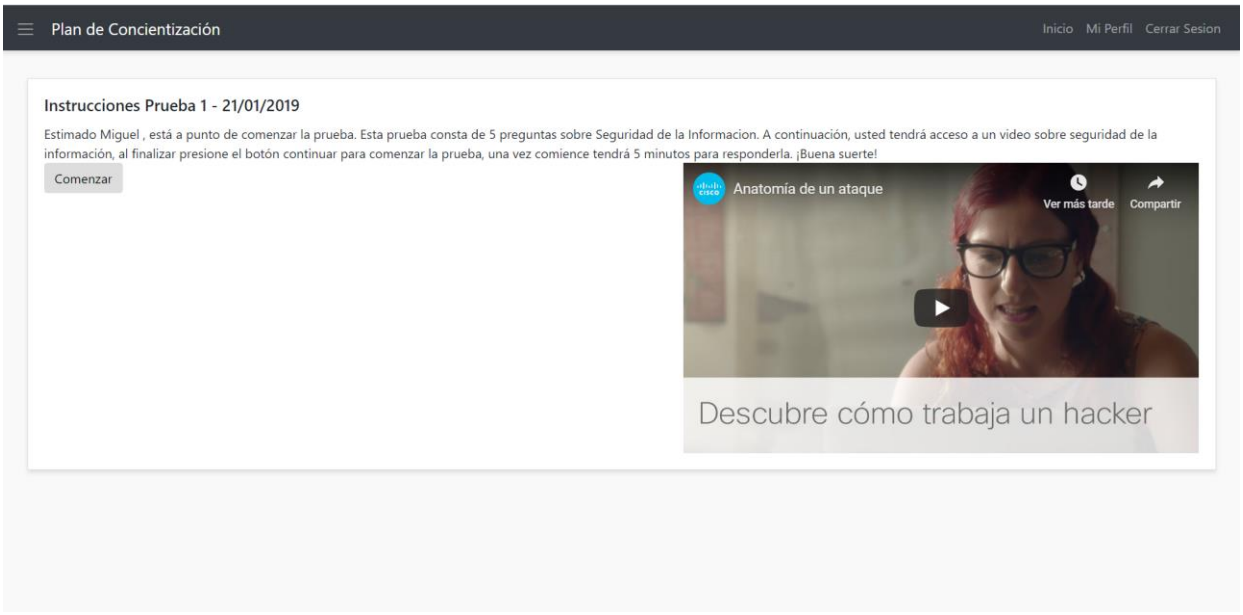
Fuente: Elaboración Propia

Figura 41 – Visualización página web(continuación)



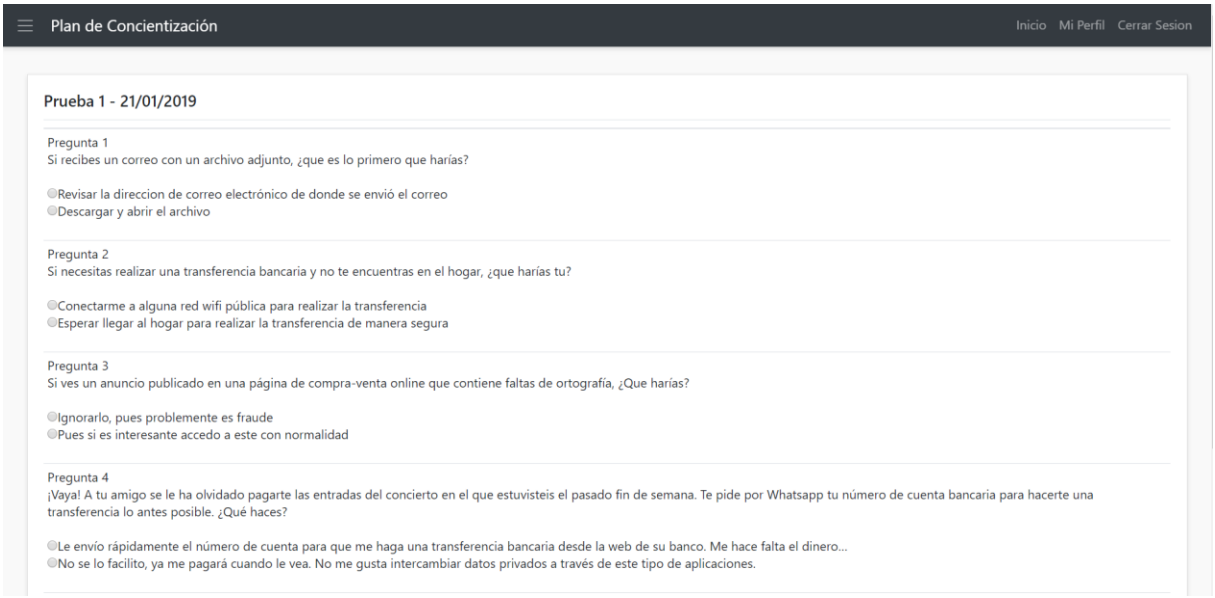
Fuente: Elaboración Propia

Figura 41 – Visualización página web(continuación)



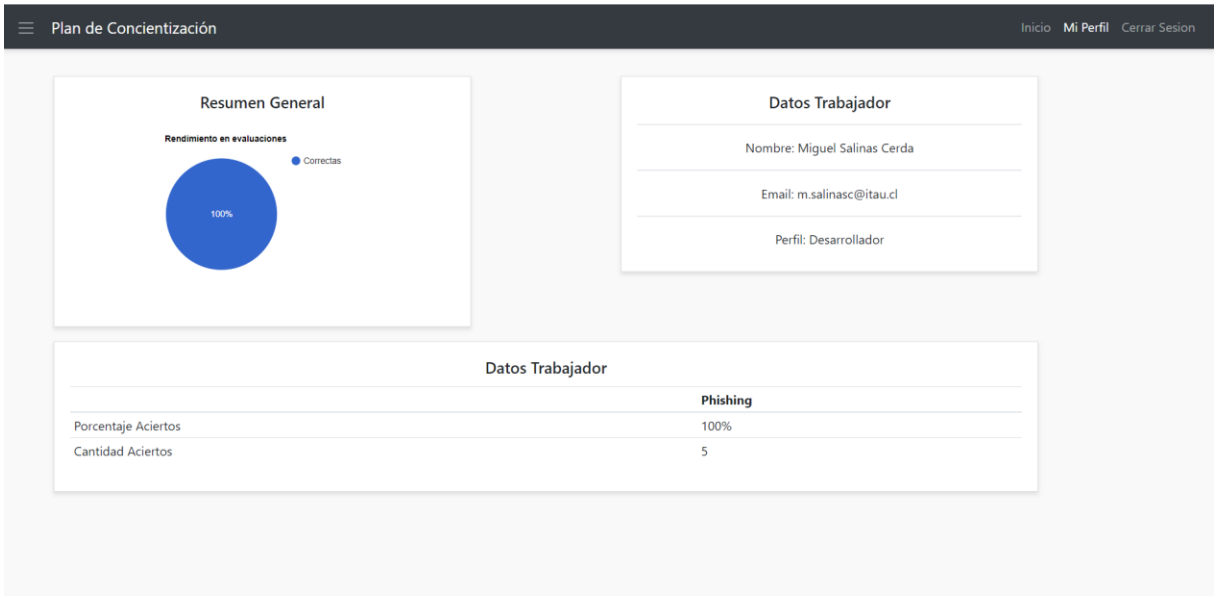
Fuente: Elaboración Propia

Figura 41 – Visualización página web(continuación)



Fuente: Elaboración Propia

Figura 41 – Visualización página web(continuación)



Fuente: Elaboración Propia