UNIVERSIDAD CENFOTEC

MAESTRÍA EN CIBERSEGURIDAD

CREACIÓN DE UNA PLATAFORMA WEB SEGURA, PARA AUTOMATIZAR EL MODELO DE MADUREZ EN CIBERSEGURIDAD ECM2 CON EL FIN DE FACILITAR LA TAREA DE DETERMINAR EL ESTADO REAL EN MATERIA DE CIBERSEGURIDAD A INSTITUCIONES SIN IMPORTAR SU TAMAÑO O SECTOR

DOCUMENTO FINAL DEL PROYECTO DE INVESTIGACIÓN APLICADA 2

Estudiantes:

Soto Elizondo Marlon

Pérez González Luis Humberto

Septiembre, 2018

Declaratoria de derechos de autor

Dedicatoria

Este trabajo final de graduación se la dedico a los seres que me dieron la vida: Luis Ángel Pérez y Sonia María González, gracias a ellos y a su apoyo, siempre incondicional, tuve la sabiduría y fortaleza para llegar hasta aquí. También a Marlen Rojas, ella junto a Sebastián, fueron el motor y la motivación para alcanzar esto.

Humberto

Dedico mi trabajo y esfuerzo a mi mamá, Elida Elizondo Arias; a mi papá, Jacinto Soto Espinoza, porque fueron las personas que me formaron. A mis hermanos, Minor, Michael y Jesús, que siempre me han apoyado. También a Montserrat Cruz y mi hijo Elías, pues su presencia incentivó mi labor para llegar a la meta. Mi éxito les pertenece.

Marlon

Agradecimientos

Agradecemos profundamente:

Al personal del MICITT y al CSIRT-CR, en especial a Johnny Pan, por la confianza depositada; sus valiosos aportes hicieron posible este proyecto.

A Radiográfica Costarricense S.A, y al personal del proyecto SICOP, por la autorización para el uso del componente de firma digital en el proyecto.

A nuestros profesores de carrera, porque su conocimiento y ardua labor nos dieron las bases de aprendizaje para lograr cumplir con este cometido.

A Xenia Guerrero Arias, su conocimiento, experiencia y visión lograron una mejor versión de este proyecto.

A nuestro tutor, Ingeniero Msc. Cesar Rodríguez Bravo, por su paciencia y la orientación constante.

A compañeros y amigos, por darnos palabras de aliento y soñar con nosotros.

A todas aquellas personas que, de una u otra forma, hicieron aportes a nuestro trabajo de graduación.

Humberto y Marlon

Hoja de firmas

Documento final del Proyecto de Investigación Aplicada 2 a nivel de Maestría en Ciberseguridad correspondiente a los estudiantes: **Luis Humberto Pérez González y Marlon Soto Elizondo**, fue aprobado por el siguiente Tribunal Examinador:

_____	_____
Msc. Cesar Rodríguez Bravo	**Msc. Ignacio Trejos Zelaya**
Tutor	Tribunal Examinador

_____

Mag. Xenia Guerrero Arias

Lector Externo

Con la NOTA: _____

UNIVERSIDAD CENFOTEC

San José, Costa Rica

Septiembre, 2018

Tabla de Contenido

Índice de figuras

.....

Índice de tablas

Glosario

CLR: (Lista de revocación de certificados digitales) Es una lista de certificados que ya no son válidos y en los que ningún sistema debe confirmar.

CSIRT-CR: Centro de Respuesta de incidentes de seguridad Informática, del Ministerio de Ciencia, Tecnología y Telecomunicaciones.

ISACA: (Information Systems Audit and Control Association) Es una asociación internacional sin fines de lucro, conformada por profesionales que apoyan el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control de sistemas de información.

MICITT: Ministerio de Ciencia, Tecnología y Telecomunicaciones (Costa Rica).

OCSP: Protocolo de comprobación del estado de un certificado en línea, es un método para determinar el estado de vigencia de un certificado mediante la consulta a la autoridad certificadora.

OWASP: (Open Web Application Security Project) Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. Este proyecto es gestionado y apoyado por la fundación OWASP y la comunidad, la cual está conformada por empresas, organizaciones educativas y particulares de todo el mundo.

PNCTI: Plan Nacional de Ciencia, Tecnología e Innovación.

RACSA: Radiográfica Costarricense S.A.

SICOP: Sistema integrado de compras públicas.

TI: (Tecnologías de información) es un término que refiere al uso de equipos de telecomunicaciones y computadoras para el procesamiento, almacenamiento y transmisión de información.

XSS: (Cross-site scripting) es una vulnerabilidad o fallo de seguridad en aplicaciones web, que puede permitir a un tercero inyectar código JavaScript u otro lenguaje similar en la paginas web. Este tipo de ataque puede ser usado para robar información delicada, secuestrar sesiones de usuario, o redirigir al usuario a otro sitio.

XXE: (Xml External Entity) es un tipo de vulnerabilidad que se produce en las aplicaciones en donde se manipula XML. Ahí un atacante puede alterar la entrada

de un documento XML que espera la aplicación para otros propósitos, como alterar u conseguir información o ejecutar comandos que consuman recursos en exceso y afectar el funcionamiento de la aplicación.

Yii2: “Yii es un framework de PHP de alto rendimiento, basado en componentes para desarrollar aplicaciones web modernas en poco tiempo” (www.yiiframework.com, 2018).

Resumen

La ciberseguridad es una de las áreas que más preocupa a las diferentes organizaciones en la actualidad, la cantidad de ataques a los sistemas de información, así como la diversificación en los mecanismos para cometerlos van en aumento. Las compañías, principalmente de mayor tamaño y con más recursos económicos, están invirtiendo más en seguridad; sin embargo, las de menor tamaño ven limitadas sus posibilidades, ya que en muchos casos ni siquiera saben por dónde empezar. Es aquí donde los modelos de madurez en ciberseguridad juegan un papel importante, ya que permiten a las organizaciones identificar sus fortalezas y debilidades en la materia, facilitando la labor de priorizar recursos y esfuerzos.

A nivel nacional, el Centro de Respuesta de Incidentes de seguridad Informática (CSIRT-CR) del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) es el ente encargado de velar por los asuntos relacionados a la seguridad informática y cibernética. Sin embargo, cuenta con recursos limitados, y no dispone de una herramienta que les permita identificar el estado real de la ciberseguridad, principalmente en las instituciones de gobierno.

El presente trabajo se enfoca en la “Creación de una plataforma web segura, para la automatización del modelo de madurez en ciberseguridad ECM2, la cual busca facilitar la tarea de determinar el estado real de la ciberseguridad en las organizaciones, sin importar el tamaño o sector”. Como patrocinador y principal beneficiario del proyecto, está el CSIRT-CR, por lo que se pretende que la herramienta sea de gran ayuda en el proceso de toma de decisiones, y determinar las acciones para el fortalecimiento de la ciberseguridad en el país por parte de este ente.

Para la construcción del proyecto, se usa como base el modelo de madurez, desarrollado por el Ingeniero Msc. Cesar Rodríguez Bravo, el cual es plasmado en una aplicación web, construida utilizando buenas prácticas de seguridad, tanto en código fuente, base de datos, como en la configuración de servidores. Todo este desarrollo se lleva a cabo bajo tecnologías de software libre, y el uso de certificados de firma digital, como mecanismo de seguridad de la aplicación.

Capítulo 1. Introducción

1.1 Generalidades

Mediante el desarrollo de este proyecto, se pretende brindar a diferentes organizaciones sin importar tamaño o sector; una herramienta web, que permita de forma automatizada y en tiempo real, realizar una evaluación del estado actual en materia de ciberseguridad. Para ello se toma como marco de referencia el modelo de madurez en ciberseguridad ECM2, desarrollado por el Ingeniero Msc. Cesar Rodríguez Bravo, como parte de su trabajo de tesis de graduación en la Maestría de Ciberseguridad de la Universidad Cenfotec, y de quien se tiene autorización para dicha implementación.

Como primera institución interesada y además patrocinadora del proyecto, se cuenta con el apoyo del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), quienes actualmente no cuentan con datos e información real y actualizada respecto al nivel de madurez en ciberseguridad de las entidades del gobierno, y tampoco se tiene una herramienta que pueda facilitar el acopio de dicha información.

1.2 Antecedentes del problema

La seguridad de la información y de los sistemas de información de las organizaciones no es un tema reciente, por cuanto desde la creación y comercialización de las primeras computadoras, se dieron los primeros ataques informáticos y con ellos se hicieron famosos los primeros "*hackers*", entre los que destacan nombres como Steve Wozniak, cofundador de Apple y quien realizó ataques a sistemas telefónicos con el objetivo de realizar llamadas de forma gratuita. Asimismo, John Draper, conocido también como "*Captain Crunch*", fue el creador de la llamada "caja azul", un dispositivo capaz de *hackear* los sistemas telefónicos de la época, mediante la reproducción de los diferentes tonos utilizados

por las compañías telefónicas con lo cual se podían realizar llamadas de forma gratuita.

Además, cabe mencionar a Kevin Mitnick, considerado por muchos el mayor *hacker* de la historia, quien junto a dos amigos logró acceder de forma física a las oficinas de COSMOS de la compañía Pacific Bell, dicho sistema era encargado de controlar el registro de llamadas de compañías telefónicas norteamericanas. En 1983 desde una computadora en la Universidad del Sur de California ingresó a un sistema informático del Pentágono por medio de ARPA Net por lo que fue condenado a seis meses de cárcel. El FBI lo capturó en 1995 y fue condenado a prisión bajo estrictas medidas de seguridad e incluso se le prohibió hacer uso de teléfonos debido a su "peligrosidad".

Del mismo modo, el problema de los ataques informáticos se acrecentó con la creación y comercialización de las computadoras personales, así como con la popularización de Internet, la cual vino a revolucionar la forma en cómo las personas se comunican y hacen negocios. Sin embargo, dicha evolución también ha supuesto un aumento en la cantidad y complejidad de los ataques. En la actualidad se pueden encontrar diferentes tipos de ataques como son los de denegación de servicio o DoS (*Denial of Service*), los cuales consisten en un ataque a una computadora, red, servicio o recurso de manera que este, se vuelva inaccesible para los usuarios legítimos; esto provoca una pérdida de conectividad de la red o una sobrecarga de recursos del sistema. También existen los ataques de día cero los cuales consisten en explotar vulnerabilidades de sistemas de información antes de que se conozcan o sean reparadas. Otro tipo de ataque muy popular es el de "*Man in the middle*", en el cual el atacante adquiere la capacidad de leer, insertar y modificar a voluntad un mensaje entre dos o más víctimas sin que estas se den cuenta de lo que ocurre.

Es importante destacar que dichos embates pueden afectar tanto a usuarios domésticos como a grandes empresas, un ejemplo de ellos es el ataque sufrido por la empresa Target en el año 2013, donde la información personal (nombre,

dirección, teléfono, email, entre otros) y números de cuenta bancarios y tarjetas de crédito de aproximadamente 110 millones de clientes fue sustraída. En el caso de las personas, los ataques se dan principalmente por medio de técnicas como ingeniería social y *phishing*.

En Costa Rica la situación no es diferente, los sistemas de información y comunicación son parte importante del quehacer de las compañías y personas, y los ataques para tratar de alterar u obtener información confidencial o sensible, o bien inhabilitar sistemas, productos y servicios informáticos, son cada vez más frecuentes. Las grandes empresas transnacionales generalmente invierten en mecanismos de software; como antivirus, *antimalware, antispyware*, entre otros, y de *hardware*; como por ejemplo *firewalls*, servidores *proxy*, cámaras de seguridad, mecanismos de autenticación y acceso a edificios, para tratar de mantener la seguridad de sus sistemas. Sin embargo, para las pequeñas y medianas empresas, así como instituciones públicas, el tema de la seguridad es bastante nuevo y complejo, y en muchos casos no se tiene una idea de por dónde empezar.

Es así como, para Javier Cortés, las grandes compañías son conscientes del riesgo que enfrentan al manejar su información por medio de dispositivos tecnológicos como computadoras e internet, lo cual se traduce, en una mayor inversión en ciberseguridad. El mismo autor señala que “la inversión de las empresas con menos de 250 empleados en ciberseguridad es inversamente proporcional al riesgo que tienen de ser atacadas” (Cortés Domínguez, 2017). El autor señala que, por ejemplo, en el caso de España, según datos del Instituto Nacional de Ciberseguridad, para el año 2017 el 70% de aproximadamente 115 000 ataques informáticos, estuvieron dirigidos a Pymes, y que en el año 2015 una de cada tres Pymes fue atacada. El principal argumento utilizado por las pequeñas y medianas empresas es que los piratas informáticos prefieren atacar grandes compañías porque la información de estas les parece más relevante.

En lo que respecta al marco legal, desde el año 2000 se han venido desarrollando iniciativas del gobierno con el fin de promover la seguridad de la información, lo cual ha derivado en la creación de algunas leyes:

- Ley de la Administración Financiera de la República y Presupuestos Públicos (Asamblea Legislativa de la República de Costa Rica, 2001).En los artículos 110 y 111, se establecen responsabilidades para quienes afecten el desempeño de sistemas de software y/o hardware de la Administración Financiera y de Proveeduría de la República y los presupuestos de carácter público.
- Ley de Certificados, Firmas Digitales y Documentos Electrónicos y su Reglamentos (Asamblea Legislativa de la República de Costa Rica, 2005), en la cual se establecen las pautas para el uso de firma digital con el fin de dar validez a los documentos electrónicos, y asegurar la autoría de los mismos por parte del firmante.
- Ley de protección de la niñez y la adolescencia frente al contenido nocivo de internet y otros medios electrónicos (Asamblea Legislativa de la República de Costa Rica, 2011). Esta ley trata de proteger a niños y adolescentes que utilicen Internet u otros medios electrónicos en establecimientos públicos, de sitios con contenido nocivo, como pornografía, violencia, construcción de armas, consumo de drogas, entre otros.
- Ley de protección de la persona frente al tratamiento de sus datos personales (Asamblea Legislativa de la República de Costa Rica, 2011). Esta ley tiene como objetivo garantizar que se respete la autodeterminación informativa de la persona respecto a su vida privada, y se garantice el tratamiento adecuado y responsable de sus datos ya sea de forma manual o automatizada.
- Código Penal Ley 9048 Reforma de varios artículos y modificación de la sección VIII, denominada Delitos Informáticos y Conexos, del título VII del Código Penal (Asamblea Legislativa de la República de Costa Rica). Mediante estas reformas se establecen penas para quienes cometan delitos

como: violación de correspondencia o comunicaciones, violación de datos personales, extorsión, estafa informática, daño informático, espionaje, sabotaje informático, suplantación de identidad, instalación o propagación de programas informáticos maliciosos, suplantación de páginas electrónicas, facilitación de delito informático, entre otros.

Además de las leyes mencionadas se han promulgado algunos decretos ejecutivos que de igual forma buscan fomentar la seguridad de los activos de información, principalmente en las entidades públicas; algunos de ellos son:

- Decreto N°30151-J (Presidente de la República y Ministerio de Justicia y Gracia, 2002), relacionado a la prevención del uso de software ilegal en las instituciones gubernamentales, así como la autorización para el uso de software de código abierto.
- Decreto Nº32083, Comisión Internet Costa Rica (CI-CR) (Presidente de la República y Ministerio de Ciencia y Tecnología, 2004), con el fin de recomendar políticas y estrategias relacionadas al adecuado uso y desarrollo de Internet en Costa Rica.
- Decreto N°36274, Creación de la Comisión Nacional de Seguridad en Línea (Poder Ejecutivo, Ministerio de Ciencia y Tecnología, 2010), como un órgano multidisciplinario conformado por representantes; tanto de entidades públicas como privadas, con el objetivo de diseñar políticas para el adecuado uso de Internet y las tecnologías de información en el país, además de participar en la elaboración del Plan Nacional de Seguridad en Línea.
- Decreto N°37052 Creación del “Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR)” (Poder Ejecutivo, Ministerio de Ciencia y Tecnología, 2012), como ente encargado de coordinar lo relacionado a materia de seguridad informática y cibernética, así como crear un equipo de expertos en seguridad en tecnologías de información encargado de prevenir y responder ante incidentes de seguridad cibernética en las entidades del gobierno.

No obstante, a pesar de que se vienen realizando esfuerzos desde hace varios años, el tema de la ciberseguridad está cobrando mayor relevancia actualmente, donde el uso de medios informáticos para cometer delitos es más frecuente.

Según datos del informe Tendencias de Seguridad Cibernética en América Latina y el Caribe para la Organización de Estados Americanos, las autoridades costarricenses hablan de un limitado número de casos de ataques cibernéticos reportados para el año 2014, se habla de aproximadamente 600 casos, de los cuales en unos 300 se dio la apertura de un proceso formal por parte de las autoridades competentes (Symantec, 2014). Esta apertura de procesos legales no se habría podido concretar sin un avance en materia legal, como el que ha venido experimentando poco a poco el país; ello ha impactado de forma positiva, pues tanto empresas como personas sienten que existe un respaldo legal en el cual se pueden apoyar, en caso de sufrir un ataque cibernético.

1.3 Definición y descripción del problema

En la actualidad uno de los desafíos más grandes que enfrentan muchas organizaciones en nuestro país, principalmente pequeñas y medianas empresas, es la limitada cantidad de recursos económicos que poseen para invertir en rubros que no sean estrictamente relacionados con su giro de negocio. Dicha limitación incide directamente en la posibilidad que tienen, para adquirir o desarrollar herramientas que permitan evaluar de manera integral la ciberseguridad.

En el caso de CSIRT-CR el panorama es muy similar, pues el presupuesto económico con el que cuenta, así como las herramientas para la evaluación de la ciberseguridad en todas las instituciones del gobierno es limitado, ello dificulta contar con un panorama real del estado de la ciberseguridad en el aparato estatal, lo cual repercute al momento de la toma de decisiones relacionadas con este tema.

El modelo de madurez de ciberseguridad ECM2 viene a suplir esa necesidad, y se convierte en una herramienta para el análisis de la seguridad, sin embargo, dicho

instrumento también posee una dificultad, la cual consiste en la implementación y recolección de la información de manera eficiente. Ante tal situación, se vuelve una necesidad automatizar el modelo de manera que sea sencillo el poder aplicar el instrumento a las organizaciones y contar con los datos de la evaluación de manera instantánea, haciendo uso de una herramienta de acceso web, con altos estándares de seguridad. Dichas evaluaciones deben ser prácticas y confiables, tanto para entidades u organizaciones privadas de cualquier tamaño, como para entidades del gobierno; en el caso de estas últimas facilitan al CSIRT-CR un panorama más claro del estado de la ciberseguridad en esas instituciones, lo cual brinda un importante insumo al momento de priorizar y tomar decisiones en materia de seguridad informática, lo cual solventa el problema del desconocimiento de puntos de mejora y permite aplicar las medidas necesarias para subsanarlas.

1.4 Justificación

Actualmente muchas organizaciones, principalmente pequeñas y medianas, no cuentan con suficientes recursos económicos para invertir en la evaluación de la seguridad de sus sistemas de información, o bien, consideran que puede representar un gasto innecesario pues no sienten que pueden llegar a ser blanco de un ataque cibernético.

Para estas organizaciones e incluso para otras de mayor tamaño, es de gran provecho una herramienta web segura, que les permita realizar una evaluación en materia de ciberseguridad, en tiempo real, y les brinde una retroalimentación para apoyar el proceso de toma de decisiones, en cuanto a medidas de seguridad de sus sistemas de información y comunicación.

En el caso específico del MICITT, y más concretamente el CSIRT-CR, el cual es, por decreto N°37052, el ente encargado de coordinar lo relacionado a materia de seguridad informática y cibernética de las instituciones del gobierno en el país, este realiza esfuerzos para contar con el personal y las herramientas necesarias para cumplir con dicha labor.

Esta institución actualmente no posee información para determinar el nivel en materia de ciberseguridad de las instituciones del gobierno, por lo cual es sumamente complicado tomar las medidas correctivas y preventivas necesarias, tanto a nivel general como específico para cada entidad.

La automatización de una herramienta para que cada institución de gobierno mida su nivel de madurez en ciberseguridad, va a proporcionar al CSIRT-CR información real del estado de la ciberseguridad en cada una de estas instituciones, y del gobierno a nivel general, lo cual facilita a dicho ente enfocar sus esfuerzos y recursos en atacar los aspectos de la ciberseguridad en los que se detecten mayores carencias.

El hecho de contar con una herramienta automatizada tiene ventajas tanto para el CSIRT-CR, como para las instituciones del gobierno que se autoevalúen, entre las que destacan:

- No es necesario que personal del CSIRT-CR se desplace a cada institución para facilitar la herramienta de evaluación. De igual forma, tampoco es necesario que la institución envíe personal con dicha evaluación completada, ya que la herramienta estaría disponible en línea para su uso.
- No es necesario que personal del CSIRT-CR invierta tiempo tabulando o pasando a formato digital la información recopilada en cada una de las instituciones.
- Cada institución puede ver de forma práctica y gráfica el resultado de su evaluación en el modelo de seguridad ECM2, y cuáles son los aspectos del modelo en los que tiene mayor fortaleza y en los que hay deficiencias.
- Personal de CSIRT-CR puede ver de forma práctica y gráfica el resultado de las evaluaciones del modelo de ciberseguridadECM2 para cada una de las instituciones del gobierno que la realicen. Además, puede tener un panorama global del estado de la ciberseguridad del conjunto de instituciones del gobierno según dicho modelo.

Con esto se busca una mayor eficiencia en el proceso de toma de decisiones acerca de las principales medidas para atacar los problemas de ciberseguridad, tanto para los encargados de cada institución, como para el personal del CSIRT-CR.

1.5 Viabilidad

El proyecto es viable debido a que se cuenta con varios elementos que hacen factible el proyecto entre los que destacan, que se cuenta con la autorización y colaboración del Ingeniero Msc. Cesar Rodríguez Bravo, quien fue el creador del modelo de madurez ECM2.

En el aspecto técnico los estudiantes cuentan con conocimientos en seguridad, sólidas bases y experiencia en cada parte del ciclo de vida de las aplicaciones web, además se cuenta con el compromiso de colaboración por parte del CSIRT-CR nacional y del MICITT.

Desde la perspectiva económica, el proyecto es viable debido a que no hay un costo económico asociado a la utilización del modelo de madurez ECM2, y para el desarrollo de la aplicación web se utilizarán tecnologías Open Source, las cuales no representan un costo para los estudiantes ni para las diferentes organizaciones que puedan hacer uso de las herramientas de evaluación. Además, al ser un proyecto de índole académico no genera un gasto adicional a ninguna institución.

Por otra parte, se cuenta con patrocinio para la implementación de la herramienta, en un *hosting* que permite que esté disponible para cualquier organización en cualquier momento sin importar ubicación geográfica. También se cuenta con el patrocinio del CSIRT-CR para la implementación de la aplicación en el MICITT, con el fin de evaluar instituciones del sector público.

1.5.1 Punto de vista técnico.

Desde el punto de vista técnico se cuenta con los conocimientos necesarios para poder diseñar, desarrollar e implementar la aplicación web.

Además, se cuenta con el apoyo del tutor del proyecto y creador del modelo ECM2 el Ingeniero Msc. Cesar Rodríguez Bravo. Así como del personal técnico del CSIRT-CR.

En cuanto a las herramientas necesarias para la elaboración e implementación del proyecto, se eligieron tecnologías de Código abierto, alineadas a estándares de desarrollo web ágil y seguro, sobre las cuales hay suficiente información y documentación para un adecuado desarrollo.

1.5.2 Punto de vista operativo.

La realización del Trabajo Final de Graduación no debe afectar de ninguna manera el día a día de la organización patrocinadora, debido a que los estudiantes no necesitan acceso a ningún recurso físico de la organización.

Una vez finalizado el proyecto este tampoco debe significar una interferencia en las actividades diarias de las instituciones diagnosticadas, por el contrario, la retroalimentación de esta herramienta debe servir como un insumo para la prevención, detección, corrección de problemas de seguridad en estas.

1.5.3 Punto de vista económico.

Desde el punto de vista económico el proyecto es viable, pues no representa un costo económico para ninguna organización, pública o privada, que quiera hacer uso de la aplicación, esto porque el desarrollo provisto por los estudiantes, se realiza de manera *ad honorem*. Asimismo, se cuenta con la autorización del Ingeniero Msc. César Rodríguez Bravo para utilizar el modelo de seguridad ECM2 sin costo económico alguno.

En cuanto a las licencias de software para el desarrollo de la aplicación, se utiliza software libre, razón por la cual, estas no deben representar un cargo económico para los estudiantes, ni tampoco para las organizaciones que vayan a hacer uso de la aplicación para evaluar la ciberseguridad.

En este sentido, se va a proveer al CSIRT-CR una solución web sin costo económico, que cubre algunas de sus necesidades en cuanto al panorama de la

ciberseguridad en las instituciones del estado, lo cual les permite reorientar de forma más eficiente los recursos.

Adicionalmente, con el proyecto se van a ver beneficiadas muchas otras organizaciones, las cuales van a poder ser evaluadas y recibir retroalimentación en tiempo real, mediante una aplicación web segura, con ello se brinda información de primera mano para la toma de decisiones y por tanto disminuir la probabilidad de ocurrencia de eventos de ciberseguridad, así como su impacto, lo que se traduce en una disminución de los recursos y tiempo.

1.6 Objetivos

Se ha seleccionado la taxonomía de Benjamin Bloom ya que es utilizada como estándar en el sistema educativo costarricense, lo cual supone un gran número de fuentes de información en las cuales apoyarse, al momento de estructurar los objetivos de una investigación.

1.6.1 Objetivo general.

- Crear una plataforma web segura para automatizar el modelo de madurez en ciberseguridad ECM2 con el fin de facilitar la tarea de determinar el estado real en materia de ciberseguridad a instituciones sin importar su tamaño o sector.

1.6.2 Objetivos específicos.

- Conocer a detalle el modelo de madurez en ciberseguridad ECM2 que se quiere automatizar para la evaluación del nivel de seguridad en instituciones sin importar su tamaño o sector.

- Identificar las mejores prácticas en seguridad de aplicaciones, servidores y bases de datos, con el fin de desarrollar una aplicación web que permita la

evaluación del nivel de ciberseguridad en diversas organizaciones y cumpla con estándares en la materia.

- Investigar cómo trabaja el proceso de autenticación de usuarios en un sistema web mediante el uso de firma digital, con el objetivo de fortalecer el nivel de seguridad en la autenticación de los usuarios de la herramienta.

- Elaborar la arquitectura de la solución para la automatización del modelo de madurez en ciberseguridad ECM2 que refleje el uso de estándares de seguridad estudiados durante la Maestría en Ciberseguridad.

- Desarrollar una aplicación web segura que permita aplicar el modelo de madurez en ciberseguridad ECM2 en diferentes organizaciones sin importar su tamaño y sector.

- Aplicar las mejores prácticas de seguridad en aplicaciones, servidores y bases de datos identificadas, con el fin de elaborar una herramienta de evaluación del nivel de seguridad que cumpla con medidas de seguridad estudiados durante la Maestría en Ciberseguridad.

- Realizar pruebas funcionales y de seguridad de la aplicación, que permitan determinar si esta cumple con los requerimientos para la evaluación del nivel de seguridad de las instituciones, así como las mejores prácticas en materia de seguridad para el desarrollo de aplicaciones seguras.

1.7 Alcances y limitaciones

1.7.1 Alcances.

El proyecto tiene como meta el desarrollo de una aplicación web, mediante la cual se automatice el modelo de madurez en ciberseguridad ECM2 utilizando estándares de seguridad en aplicaciones web, base de datos y servidores.

Para el desarrollo del proyecto se contará con el patrocinio del CSIRT-CR, el cual se compromete a proporcionar a los estudiantes lo siguiente:

- Asesoría técnica en cuanto al uso e implementación de la firma digital.
- Apoyo técnico en la configuración y aseguramiento de servidores
- Un *hosting* adecuado para la instalación de la aplicación web.

Por tal motivo al finalizar el proyecto, el patrocinador obtendrá los siguientes productos:

- Casos de uso
- Diagramas de secuencia
- Modelo de base de datos
- Diccionario de datos
- Aplicación web funcional
- Manual de usuario
- Copia digital del documento de tesis
- Una capacitación

Es importante señalar que a pesar de ser el MICITT por medio del CSIRT-CR, la institución patrocinadora, el modelo y la aplicación son abiertos por lo cual el uso y distribución de la aplicación no es exclusivo de esta entidad. Esto permite su uso en cualquier organización, sin importar el tamaño o sector.

1.7.2 Limitaciones.

El proyecto se limita al desarrollo de una aplicación web, que permite automatizar el modelo de madurez en ciberseguridad, de acuerdo con los requerimientos iniciales, los estudiantes no adquieren el compromiso de realizar futuras ediciones o agregar nuevos requerimientos a la edición actual.

Asimismo, los estudiantes solo proveerán conocimiento técnico para la elaboración del proyecto, los ambientes para la implementación del producto deben ser proporcionados por el patrocinador.

Por lo demás, la implementación del componente para autenticar la firma digital es para uso exclusivo del CSIRT-CR. Por tal motivo se implementará otra versión de la aplicación abierta con otro mecanismo de autenticación, disponible para cualquier organismo.

1.8 Marco de referencia organizacional y socioeconómico

1.8.1 Historia.

El Ministerio de Ciencia y Tecnología se estableció en 1986 en un primer periodo como un Programa Nacional de Ciencia y Tecnología 1986-1990, durante este periodo se estructuró el Sistema Nacional de Ciencia y Tecnología, integrado por el conjunto de instituciones cuyas actividades se enmarcan en el campo de la ciencia y la tecnología, se incrementó sustancialmente la inversión en actividades de investigación y desarrollo.

En el segundo período, 1990-1994 orienta su quehacer a obtener un mayor dominio sobre las tecnologías adquiridas, en donde la ciencia y la tecnología permitieron lograr un mayor grado de eficiencia y eficacia en el sector público, aumentando a su vez la competitividad y crecimiento del sector productivo nacional. A principios de este periodo, se promulga la Ley 7169 de Promoción del Desarrollo Científico y Tecnológico y se incorpora a la cartera de Ciencia y Tecnología, mediante modificación a la Ley General de Administración Pública.

En la tercera etapa, 1994-1998, el Ministerio de Ciencia y Tecnología, impulsa un planteamiento estratégico que se dirige al fomento y apoyo del desarrollo de la competitividad en el país, y se sustenta en el Plan Nacional de Ciencia, Tecnología, Calidad, Productividad e Innovación "Hacia un desarrollo nacional sostenible orientado por los nuevos requerimientos de competitividad y las necesidades nacionales", donde el consenso, la interacción y el trabajo grupal entre los sectores, gestó un nuevo enfoque político y organizacional.

En la cuarta etapa, 1998-2002, el Ministerio ha liderado los planteamientos emitidos en el "Programa Nacional de Ciencia y Tecnología: Por el conocimiento hacia el Desarrollo" y principalmente en los últimos años, ha centrado su accionar en el desarrollo de las Tecnologías de información y de las Telecomunicaciones como instrumentos por excelencia de la transformación de la sociedad y el desarrollo económico del país.

El nivel alcanzado por el Ministerio de Ciencia y Tecnología, en los diferentes periodos desde su creación, ha sido posible principalmente por la acción coordinada con los sectores privados, académico y público y plantea los diferentes programas que constituyen el accionar del Ministerio.

A partir del 30 de enero de 2012, el Viceministerio de Telecomunicaciones pasa a ser parte del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). De esta forma se cumple con uno de los compromisos de la señora Presidenta de la República Laura Chinchilla, quien a inicios del 2010 planteó la necesidad de trasladar el Viceministerio de Telecomunicaciones hacia una institución con objetivos y responsabilidades más afines.

Durante la administración 2014-2018 se han promulgado el Plan para el Desarrollo de las Telecomunicaciones (PDT) y el Plan Nacional de Ciencia, Tecnología e Innovación (PNCTI), enmarcados dentro del Plan Nacional de Desarrollo Alberto Cañas Escalante (PND 2015-2021). Ambos planes pretenden un modelo de desarrollo mediante la senda del conocimiento y la innovación, cuyo fin es forjar una visión a nivel país más competitiva y mejor conectada con la dinámica global actual.

1.8.2 Tipo de negocio y mercado meta.

El Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) es una entidad estatal que busca regular, promover y fomentar condiciones favorables para la investigación, la innovación, el conocimiento, y la tecnología en el país.

1.8.3 Misión, visión.

Misión

"Dictar la política pública de ciencia, tecnología y telecomunicaciones, que permita al país potenciar el aprovechamiento del conocimiento y la innovación, para priorizar y dirigir las iniciativas del sector hacia la competitividad, el bienestar y la prosperidad" (Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2017).

Visión

"Ser el propulsor de un modelo país de largo plazo basado en el conocimiento y la innovación para alcanzar un desarrollo integral y sustentable con liderazgo global" (Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2017).

1.9 Estado de la cuestión

Formulación de preguntas

Enfoque de la pregunta

Esta revisión se enfoca en identificar los principales modelos de madurez en ciberseguridad existentes en el mercado, y determinar cuáles se encuentran automatizados para su aplicación en una organización.

Calidad y amplitud de la pregunta

- **Problema**

Existe la necesidad de contar con una herramienta que permita determinar el nivel de madurez en ciberseguridad de diversas organizaciones, sin importar tamaño o el sector al cual pertenecen, por ello es conveniente determinar cuáles son los principales modelos de madurez en ciberseguridad utilizados actualmente en el mercado, y si existe una herramienta automatizada que facilite la aplicación y evaluación de estos en una organización.

- **Preguntas**

¿Cuáles son los principales modelos de madurez en ciberseguridad? ¿Cuáles de estos modelos están automatizados?

- **Palabras clave y sinónimos**

Cybersecurity, maturity model, capability maturity model, automated, ciberseguridad, modelo de madurez, modelo de madurez de capacidades, automatización.

- **Efecto**

Identificar los modelos de madurez en ciberseguridad más utilizados y si existe una automatización de los mismos.

Selección de fuentes

- **Métodos de búsqueda de fuentes**

El principal recurso a consultar son las bases de datos de literatura científica, las cuales aportan fuentes de información confiables y de calidad, como por ejemplo investigaciones científicas, libros, artículos de revista entre otros. Como fuente de datos primaria se utiliza Scopus (https://www.scopus.com/), la cual es una base de datos que permite realizar búsquedas avanzadas. Como segunda opción Semantic Scholar (https://www.semanticscholar.org/) un motor de búsqueda académico sin fines de lucro. Tercera opción Google Académico (https://scholar.google.com/), que de igual forma brinda información de fuentes confiables o de gran credibilidad. Además de los anteriores, se consultan libros, artículos y otras publicaciones disponibles en Internet de forma gratuita.

- **Cadena de búsqueda:**

TITLE-ABS-KEY (cybersecurity AND maturity AND model) AND (LIMIT-TO (SUBJAREA, "COMP")) AND (LIMIT-TO (EXACTKEYWORD, "Cybersecurity") OR LIMIT-TO (EXACTKEYWORD , "Maturity Model"))

TITLE-ABS-KEY (cybersecurity AND capability AND maturity AND model) AND (LIMIT-TO (SUBJAREA, "COMP ")) AND (LIMIT-TO (EXACTKEYWORD, "Cybersecurity ") OR LIMIT-TO (EXACTKEYWORD , "Capability Maturity "))

- **Lista de fuentes**

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure.

Comparative Study of Cybersecurity Capability Maturity Models.

Modelos de Madurez en Ciberseguridad: una revisión sistemática.

Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects.

Selección de estudios

- **Inclusión de estudios y definición de criterios de exclusión**

Criterios de inclusión

- Artículos con las palabras clave buscadas.
- Publicaciones o artículos que hablen sobre modelos de madurez en ciberseguridad y gestión de seguridad de la información.
- Publicaciones técnicas sobre ciberseguridad en ambientes web.

Criterios de exclusión

- Artículos de opinión personal sobre seguridad.
- Debido a lo dinámico y cambiante de la tecnología artículos mayores a 5 años se descartaron.

- Publicaciones en las cuales no se podían comprobar sus fuentes o no existía bibliografía.
- Publicaciones duplicadas.

- **Procedimientos para la selección de estudios**

Para la selección de las principales de fuentes de información se sigue el siguiente proceso:

- Se ingresa al sitio web de la base de datos de literatura científica; Scopus, Semantic Scholar, Google Académico, y se realiza una búsqueda con las palabras claves que fueron determinadas.
- Se realiza una lectura de los títulos que fueron retornados en la búsqueda y se busca que el mismo tenga una relación, o contenga las palabras claves que se definieron.
- Se realiza una lectura del resumen o abstract de cada uno de los artículos que fueron seleccionados en el paso anterior, con el fin de determinar si el contenido del mismo tiene relación con el tema.
- Se realiza una lectura rápida del contenido del artículo, dando mayor énfasis a títulos o subtítulos, cuadros de resumen, cuadros comparativos, entre otros datos que puedan brindar un mayor detalle del contenido del artículo.

- **Resumen de resultados**

Acerca de los modelos de madurez:

El concepto de “Modelo de Madurez” no es algo nuevo, en realidad una de las primeras definiciones que se conoce fue dada aproximadamente en el año de 1986, por parte del SEI (Software Enginieering Institute), quienes a solicitud del Gobierno Federal de los Estados Unidos de América iniciaron el desarrollo de un *framework* o modelo de madurez de procesos, con el fin de evaluar sus procesos de desarrollo de software y el de sus principales proveedores. Fue a partir de este *framework* que el SEI formaliza el concepto de modelo de madurez de

capacidades para Software (CMM), cuya primera versión fue publicada de forma oficial en 1991.

Debido a la gran aceptación de CMM se dio una proliferación de modelos no solo para la rama del desarrollo de software, como, por ejemplo:

- P-CMM: People CMM.
- SA-CMM: Software Acquisition CMM.
- SSE-CMM: Security Systems Engineering CMM.
- T-CMM: Trusted CMM
- SE-CMM: Systems Engineering CMM.
- IPD-CMM: Integrated Product Development CMM

Lo anterior también empezó a generar cierta confusión, por lo cual, en el año 2001, como parte de una mejora o evolución de CMM nació CMMI (Modelo de Madurez de Capacidades Integrado), el cual integra principalmente CMM-SW, SE-CMM y IPD-CMM, y que actualmente es sumamente utilizado en la industria del software.

Modelos de madurez y ciberseguridad

Como se expuso, los modelos de madurez tienen muchos años de acompañar la industria del desarrollo del software, pero ¿qué hay en relación al tema de la ciberseguridad? ¿Existen modelos para la evaluación de la madurez de la seguridad informática o la ciberseguridad?

Para entender el tema, es necesario aclarar los términos, seguridad de la información, y ciberseguridad. Para ISACA (Information Systems Audit and Control Association) capítulo Monterrey, la ciberseguridad se define como la “protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados” (Mendoza, 2015). Por lo tanto, se parte del hecho de que los sistemas de información comprenden

activos de tecnologías de información, aplicaciones, servicios, y otros componentes interconectados, con lo cual se puede inferir que la ciberseguridad se refiere a los activos de información digital.

Por otra parte, si se refiere a seguridad de la información, el concepto es más amplio, ya que la información puede encontrarse de diferentes formas o en diferentes fuentes y no exclusivamente en medios digitales, como por ejemplo de forma física (escrita o impresa), en forma no representada (en forma verbal como por ejemplo ideas); por lo tanto, se puede afirmar que la ciberseguridad es una parte importante de la seguridad de la información.

El concepto de ciberseguridad ha tomado relevancia en los últimos años, en la década de los 90 e incluso a inicios de los años 2000, el tema de la seguridad no era una prioridad para las organizaciones, los ataques cibernéticos no estaban a la orden del día como actualmente, donde prácticamente todas las empresas; principalmente las grandes corporaciones transnacionales, tienen sus sistemas conectados a internet, lo cual facilita o aumenta exponencialmente el riesgo a sufrir un ataque.

Debido al creciente número de ataques cibernéticos, un incremento de hasta un 60% de ataques en América Latina entre agosto de 2017 y 2018(Kaspersky Lab, 2018). En este sentido, los sistemas de información y comunicación han tomado gran importancia para las empresas y sus negocios y por ello la ciberseguridad ha tomado fuerza; además, los estándares así como los modelos de madurez en este aspecto han empezado a florecer.

A continuación, se realiza una reseña de los principales modelos de madurez en ciberseguridad con que se cuenta actualmente:

C2M2

Cybersecurity Capability Maturity Model (C2M2): es un modelo diseñado para ser utilizado en cualquier tipo de organización e industria, tiene como objetivo ayudar a mejorar la Ciberseguridad en las organizaciones.

El programa C2M2 está compuesto por tres modelos de madurez de capacidad de ciberseguridad: Modelo de Madurez de Capacidad de Ciberseguridad (C2M2) y dos variantes orientados a industrias específicas, Sector de electricidad (ES-C2M2) y Petróleo y Gas (ONG-C2M2) (U.S. Department of Energy (DOE), 2014).

El modelo se centra en la implementación y gestión de las prácticas de ciberseguridad asociadas con la operación y el uso de la tecnología, los activos de información y los entornos en los que operan.

NICE-CMM

La Iniciativa Nacional de Educación en Seguridad Cibernética; The National Initiative for Cybersecurity Education (NICE), es una sociedad entre el Gobierno de los Estados Unidos, universidades y el sector privado, con el objetivo de promover la educación y capacitación en materia de ciberseguridad, para lo cual han desarrollado un modelo de madurez de capacidades en ciberseguridad que se conoce como NICE-CMM (National Initiative for Cybersecurity Education – Capability Maturity Model).

Este modelo realiza una segmentación de actividades en tres áreas (Department of Homeland Security, 2014):

- Procesos y analítica: son todas las actividades que realiza una organización para la planificación de su fuerza de trabajo. Analítica representa las actividades asociadas con el uso de herramientas, modelos y métodos para la explotación de datos que ayuden a mejorar la planeación.
- Gobernanza integrada: actividades relacionadas con establecimiento de estructuras de gobierno que impulsen la toma de decisiones.
- Profesionales calificados y habilitación de tecnología: significa contar con profesionales en el campo y actividades relacionadas al uso de sistemas de información.

CERT-RMM

El modelo de gestión de la resiliencia del CERT (CERT-RMM), es un modelo de capacidades para la gestión y mejora de la resiliencia operacional. El cual se enfoca en administrar el riesgo de los activos críticos mediante la optimización de las estrategias de protección y continuidad del negocio, este no busca cambiar prácticas o comportamientos establecidos, sino evaluarlos para determinar vacíos para su posterior mejoramiento. Fue propuesto por el CERT (Computer Emergency Response Team) de la Universidad Carnigie Mellon en Estados Unidos y su desarrollo fue influenciado por el conocido CMMI, creado por la misma Universidad y otros marcos de trabajo como ITIL, COBIT, ISO-2700 (Negro)

ISO/IEC 15408

Este estándar ISO para la seguridad define dos formas de expresar los requisitos funcionales y de seguridad de TI(ISO, 2005).

- Construcción de un perfil de protección (PP) que permita crear conjuntos reutilizables de requerimientos de seguridad.
- Objetivos de seguridad (ST) definen los requerimientos de seguridad y especifica las funciones de seguridad para un producto o sistema específico que debe ser evaluados.

ISO/IEC 27001

El ISO/IEC 27001 es un estándar para la seguridad de la información, en donde se especifican algunos requisitos necesarios para establecer, implantar, mantener, evaluar y mejorar un sistema de gestión de la seguridad de la información (SGSI).

Dicho estándar se puede implementar en cualquier tipo de organización, independientemente de su tamaño o sector. Las organizaciones que implementen esta norma pueden optar por una certificación, es decir una organización independiente confirma que la seguridad de la información fue implementada cumpliendo la norma.

Está redactado por especialistas en la materia de diferentes partes del mundo, y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; es decir una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

NIST Security Maturity Levels

Es un documento guía para la evaluación de la ciberseguridad en una organización en base a cinco niveles de madurez (NIST, 2016):

- Política
- Procedimientos
- Implementación
- Prueba
- Integración

Para su aplicación, el NIST indica que “se debe evaluar el nivel de madurez para cada uno de los criterios de revisión. Un nivel de madurez más alto solo puede alcanzarse si se alcanza el nivel de madurez previo” (NIST, 2016).

ECM2

Además de los modelos de madurez de índole comercial mencionados anteriormente, se cuenta con el Modelo de Madurez en Ciberseguridad ECM2, en el cual se basa la propuesta de desarrollo de este proyecto. Dicho modelo responde a la necesidad de muchas organizaciones de contar con una herramienta que sea fácil de aplicar, ya que los modelos más conocidos y mencionados anteriormente han presentado algunos problemas de implementación para diferentes organizaciones.

El modelo de ciberseguridad ECM2 es completo por cuanto abarca las diferentes áreas y escalas que puedan tener las organizaciones.

Es fácil de comprender e implementar, ya que una persona con conocimientos en TI, sin necesidad de ser un experto en ciberseguridad, lo puede aplicar en la organización.

Una de sus principales ventajas es que no tiene los costos de implementación de los modelos de madurez conocidos y comercializados, como ISO, los cuales no son accesibles para pequeñas y medianas empresas.

Capítulo 2. Marco teórico o conceptual

El principal objetivo de este proyecto es la automatización del modelo de madurez en ciberseguridad ECM2, utilizando diferentes técnicas para el fortalecimiento de la seguridad en el desarrollo de aplicaciones web estudiadas a lo largo de la carrera; como por ejemplo la autenticación por medio de firma digital, uso de encripción de información sensible, *hardening* de servidores, entre otros, con lo cual se pueda garantizar un producto funcional, pero además robusto en la parte de seguridad en el manejo de la información de los diferentes usuarios e instituciones que puedan hacer uso de esta.

¿Qué es automatización?

Como se mencionaba anteriormente, se quiere automatizar un modelo de madurez en ciberseguridad, lo cual en este caso concreto significa pasarlo del papel a una aplicación web, aprovechando las ventajas que este tipo de aplicaciones pueden ofrecer a los usuarios, como por ejemplo, acceso desde cualquier parte del mundo, posibilidad de visualizar de forma gráfica y tabulada el resultado de las diversas evaluaciones efectuadas, reducción en el costo económico de materiales como el papel, entre otros.

El concepto de automatización según la Real Academia Española consiste en tratar de sustituir en un proceso el operador humano por dispositivos mecánicos, electrónicos o tecnológicos(Real Academia Española, 2017). Dicha sustitución se puede llevar a cabo de forma parcial o total.

Al realizar una automatización, los objetivos de esta van a ser minimizar el esfuerzo humano y mejorar la productividad de una operación y hacer un mejor uso del tiempo y recursos. Además, al automatizar el modelo se facilita la colaboración con otras instituciones debido a que estas pueden hacer uso de la herramienta y con ella obtener una noción del estado en que se encuentran y aplicar las acciones correctivas del caso y con ello minimizar el riesgo de que puedan sufrir un incidente.

Entonces, ¿En qué consiste un modelo de madurez?

Los modelos de madurez son una evolución de las prácticas para la gestión de calidad en los procesos organizacionales. Inicialmente fueron aplicados en la industria del desarrollo de software, con el desarrollo de CMM (Capability Maturity Model) por parte de la Universidad de Carnegie-Mellon para el SEI (Software Engineering Institute) a finales de los años 80.

Un modelo de madurez es

> (…) un conjunto estructurado de elementos (buenas prácticas, herramientas de medición, criterios de análisis, etc.), que permiten identificar las capacidades de una organización… compararlas con estándares existentes, identificar vacíos o debilidades y establecer procesos de mejora continua (Castellanos, Gallego, Delgado, & Merchán, 2014).

Firma Digital

Una de las medidas de seguridad que se requieren para robustecer el acceso a esta aplicación web es la autenticación mediante el uso de firma digital, dejando de lado el tradicional método mediante usuario y contraseña, con lo cual se minimiza el riesgo de que los usuarios puedan ser suplantados, en caso de no utilizar contraseñas seguras.

Se entiende la **firma digital** como un procedimiento en el cual un usuario puede autenticarse y firmar documentos electrónicos, en internet, con respaldo legal. En este:

> (…) método se asocia la identidad de una persona o equipo, con un mensaje o documento electrónico, para asegurar la autoría y la integridad del mismo. La firma digital del documento es el resultado de aplicar algoritmos matemáticos, (denominados función hash), a su

contenido y, generando una firma digital del documento (Dirección de Certificadores de Firma Digital Ministerio de Ciencia y Tecnología, s.f.).

Mediante el uso de firma digital la probabilidad de que quien se esté autenticando sea quien verdaderamente dice ser, son mayores que cuando se utilizan los métodos de usuarios y contraseña convencionales; sin embargo, cabe rescatar que parte de la seguridad depende de la adecuada custodia que el usuario le dé al dispositivo de identificación con la firma digital.

La firma digital nacional está basada en el estándar X.509 del ITU-T (International Telecommunication Union-Telecommunication Standarization Sector) y el ISO/IEC (International Standards Organization / International Electrotechnical Commission), este formato permite una validación cruzada del certificado al permitir mediante diferentes atributos comprobar su validez, como lo es el caso de la fecha de expiración, las listas de revocación (CLR) y los OCSP los cuales son un servicio en línea de comprobación del estado del certificado.

A continuación, se exponen y explican algunos otros conceptos que están relacionados directamente con el tema de ciberseguridad y desarrollo de aplicaciones web seguras y que se consideran relevantes en el marco de este documento:

Ciberseguridad

La ciberseguridad es un término que ha tomado relevancia debido a la cantidad de delitos que se cometen hoy día utilizando medios informáticos y principalmente la internet, esta última empleada como un facilitador de negocios y operaciones en las empresas, pero que ha sido usado como canal de un número elevado de delitos; tanto a empresas como personas.

Hay muchas definiciones de ciberseguridad, y muchas hacen referencia a la importancia de resguardar infraestructura computacional y los datos de sus sistemas de información. La Unión Internacional de Telecomunicaciones en su recomendación UIT-T X.1205, define el término ciberseguridad como:

> El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno (Unión Internacional de Telecomunicaciones, 2008, p.3).

Amenaza

Según el sitio oficial de ISO 27001 en Español, una amenaza es una "causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización" (ISO 27000, 2012). Partiendo de esta definición, se puede ver una amenaza como una fuente potencial de daño, un peligro latente, un "enemigo" esperando el momento propicio para causar un impacto negativo en la operativa habitual de una organización.

Las amenazas se pueden clasificar en tres tipos (Programa Sociedad de la Información y el Conocimiento PROSIC, 2012):

- La revelación de información: amenaza de que un ente no autorizado pueda acceder ciertos recursos sin autorización.
- La denegación de servicio, o repudio: cuando un ente autorizado no puede acceder a los recursos.
- La corrupción de la integridad: se da con la alteración o pérdida de información, o inserción de información falsa.

Vulnerabilidad

Cuando se habla de una vulnerabilidad las personas suelen asociarlo con una deficiencia o debilidad presenta en algo, o hacia algo. También se puede asociar a la carencia de cierto grado o características de conformidad o fiabilidad. En el campo de la seguridad informática también es común escuchar hablar de este término. El sitio web de la ISO 27001 define vulnerabilidad como una “debilidad de un activo o control que puede ser explotada por una o más amenazas” (ISO 27000, 2012).

Por su parte Voutssás M. (2010) hace referencia a una condición de debilidad presente en los recursos informáticos, la cual los hace susceptibles o propensos ante una amenaza, que puede ser explotada de forma intencional o accidental. Este autor continúa indicando que las vulnerabilidades son medidas de protección, tanto físicas como lógicas, procedimentales o legales, inadecuadas o insuficientes, y que al ser explotadas pueden causar un impacto negativo en la operativa normal de una organización, y con ello pérdidas económicas o de imagen.

Riesgo

“Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias” (ISO 27000, 2012).

La seguridad de la información tiene como objetivo minimizar los riesgos y llevarlos a niveles aceptables para el negocio, procurando que el impacto operativo y económico en caso de que se materialicen sea el menor posible. Con el fin de minimizar riesgos, las organizaciones deben establecer controles que permitan asegurar la continuidad de las operaciones del negocio.

El Programa Sociedad de la Información y el Conocimiento PROSIC (2012) apunta que, un riesgo se materializa cuando una amenaza explota una vulnerabilidad y causa un impacto en la operativa de una organización, generalmente asociado a una pérdida económica o de imagen, que en ocasiones puede ser devastador para una compañía.

Hardening

En español *hardening* se puede traducir como endurecimiento, en el caso particular de informática este endurecimiento se refiere a reforzar, mejorar, y/o maximizar las medidas de seguridad de se adoptan para proteger los sistemas y activos de información en una organización, con el fin de disminuir los riesgos de posibles amenazas ante un ataque.

Desde un enfoque un tanto más técnico, *hardening* se refiere al proceso mediante el cual se emplean una serie de "técnicas y medidas de seguridad para endurecer un sistema con el objetivo de cerrar agujeros de seguridad, eliminar servicios innecesarios y fortalecer el control de acceso para evitar en lo posible ataques que dejen el sistema funcionando de una manera incorrecta o indisponible" (Eleanor A., Diana G., Iván L., & Jenniffer M., 2017).

El principal objetivo del *hardening* es minimizar las posibilidades de que una organización sufra un ataque a sus sistemas de información, o que las consecuencias sean las menores posibles para el negocio en caso de que haya uno. En otras palabras, lo que se busca es poner un escenario difícil a un atacante, para lo cual se deben tomar medidas que permitan identificar las principales vulnerabilidades de los sistemas de información de la organización, y realizar una priorización de estas de acuerdo a los objetivos del negocio, para tomar las medidas que permitan minimizar el impacto en caso de un incidente de seguridad.

Este es un proceso de mejora continua, ya que todos los días son descubiertas y publicadas vulnerabilidades en sistemas operativos, protocolos de red, y muchos

otros productos de hardware y software que son parte esencial en las operaciones y negocios de la mayoría de organizaciones a nivel mundial.

Capítulo 3. Marco metodológico

3.1 Tipo de investigación

El tipo de investigación seleccionada para el presente trabajo es la aplicada, debido a que esta, “se caracteriza porque, busca la aplicación o utilización de conocimientos adquiridos, a la vez que se adquieren otros" (Cordero, 2009). Además, que “usa el conocimiento y los resultados de la investigación como una forma rigurosa, organizada y sistemática de conocer la realidad” (Cordero, 2009).

3.2 Alcance investigativo

El alcance de la investigación es descriptivo, debido a que su objetivo es únicamente establecer una descripción lo más completa posible sobre el estado de la seguridad en las instituciones evaluadas, para dicha evaluación se va a utilizar el modelo de madurez en ciberseguridad ECM2, como marco de referencia. El proyecto no va a tomar en cuenta las causas que originaron la situación encontrada, ni las posibles consecuencias que dicho estado le puede significar a la organización. Sin embargo, la información recopilada va ser un importante insumo para la toma de decisiones y la distribución de recursos tanto a nivel de la organización evaluada como para la organización evaluadora.

3.3 Enfoque

El enfoque de la investigación es mixto, debido a que utiliza tanto métodos cuantitativos como cualitativos y los vincula en el proceso, con el fin de poder brindarle al usuario una mejor interpretación del estado de la ciberseguridad en las instituciones donde se aplique la herramienta.

3.4 Diseño

El diseño de la investigación es secuencial, debido a que en una primera etapa se recolectan los datos cuantitativos de la evaluación, estos se hacen por cada dominio del modelo de madurez, una vez cuantificados los resultados se pasa a una segunda etapa en donde el producto de la calificación anterior sirve como

insumo para otorgar una valoración cualitativa, tanto para el dominio como para la organización en general.

3.5 Población y muestreo

Para la presente investigación, no se realizarán encuestas o la aplicación del instrumento a una determina población, sino que se orientó en el diseño de una solución de automatización del modelo de madurez en ciberseguridad ECM2, con lo cual se podrá contar con una herramienta para determinar el estado real de la ciberseguridad en las organizaciones, sin importar el tamaño o sector. La aplicación y promoción del instrumento una vez confeccionado queda a discreción de los usuarios de la herramienta y fuera del alcance de este proyecto.

3.6 Instrumentos de recolección de datos

Debido a que el modelo de madurez en ciberseguridad ECM2 ya ha sido evaluado y validado anteriormente, y que el fin del proyecto es la automatización del mismo, entonces no es necesario el realizar algún instrumento de recolección de datos tradicional como encuestas o entrevistas. Empero la aplicación se va a someter a una serie de evaluaciones de seguridad y de desempeño en donde se utilizará la observación y listas de cotejo como método para comprobar el funcionamiento esperado.

Capítulo 4. Propuesta de solución

La propuesta de solución se enfoca en la automatización del modelo de madurez en ciberseguridad ECM2, mediante el desarrollo de una aplicación web que facilite al CSIRT-CR la recopilación de información sobre el estado de la ciberseguridad en el país, sin importar, si las instituciones que se sometan a evaluación sean del sector público o privado. Además, dicha aplicación debe ser flexible para que su implementación no sea únicamente en la institución, sino que pueda ser instalada en un servidor web público el cual brinde la posibilidad a más instituciones, aunque no sean parte del foco de interés del CSIRT-CR, de verse beneficiadas con dicha herramienta y modelo de ciberseguridad.

La aplicación web debe ser amigable con el usuario, sencilla de manipular, fresca a la vista, y que refleje la esencia y funcionalidad del modelo en ciberseguridad ECM2. Además, debe ser parametrizable, de tal manera que, si dicho modelo sufre cambios o actualizaciones por parte del autor, estos se puedan incorporar sin que la herramienta vea afectada su funcionalidad.

Como punto importante, el desarrollo de la herramienta debe buscar finalmente la seguridad del producto. Por consiguiente se requiere contemplar pautas, consejos y buenas prácticas más recientes y eficientes, en materia de seguridad para desarrollo de aplicaciones web, bases de datos y servidores. En este sentido, una de las principales características será la implementación de autenticación mediante el uso de firma digital, además del uso de un *framework* para el desarrollo de aplicaciones web con características de seguridad bastante robustas como lo es Yii2.

Para lograr el desarrollo adecuado del proyecto, es necesario definir las principales actividades y consideraciones a tomar en cuenta para cumplir con cada uno de los objetivos planteados, estas se presentan a continuación:

Para cumplir con el **objetivo de conocer a detalle el modelo de madurez en ciberseguridad ECM2**, se solicita el documento de tesis con la propuesta de

dicho modelo a su autor, el Ingeniero Msc. César Rodríguez Bravo. Una vez que se cuenta con el documento, se procede a su lectura y análisis, con el fin de comprender su estructura, forma de aplicación e interpretación, para poder llevarlo a una aplicación web funcional.

Para desarrollar el objetivo de **identificar las mejores prácticas en seguridad de aplicaciones, servidores y bases de datos, con el fin de desarrollar una aplicación web que permita la evaluación del nivel de ciberseguridad en diversas organizaciones y cumpla con estándares en la materia,** se realiza una investigación con fuentes principalmente de Internet.

En el apartado de buenas prácticas para el desarrollo de aplicaciones seguras, el Open Web Application Security Project (OWASP) sin lugar a duda es una de las mejores opciones. OWASP se define en su página web como una organización benéfica sin fines de lucro 501 (c) (3) a nivel mundial enfocada en mejorar la seguridad del software. Su misión es:

> Hacer visible la seguridad del software, para que las personas y las organizaciones puedan tomar decisiones informadas. OWASP se encuentra en una posición única para proporcionar información imparcial y práctica sobre AppSec a individuos, corporaciones, universidades, agencias gubernamentales y otras organizaciones de todo el mundo. Operando como una comunidad de profesionales afines, OWASP emite herramientas de software y documentación basada en el conocimiento sobre la seguridad de las aplicaciones (OWASP).

Para el desarrollo de la automatización del modelo de ciberseguridad ECM2 se consideran principalmente las siguientes 3 herramientas del proyecto OWASP:

- **Estándar de verificación de seguridad en aplicaciones 3.0.1**: “El estándar de verificación de seguridad en aplicaciones es una lista de requerimientos de seguridad o pruebas que pueden ser utilizadas por arquitectos,

desarrolladores, testers, profesionales de seguridad e incluso consumidores, para definir tan segura es una aplicación" (OWASP).

- **The OWASP ZedAttack Proxy (ZAP)**: Según la página oficial de OWASP, esta es una aplicación gratuita que ayuda a evaluar de forma automática muchos aspectos de la seguridad de aplicaciones web, lo que permite identificar vulnerabilidades en estas. Es una herramienta sumamente utilizada por personas dedicadas a realizar pruebas de penetración.
- **OWASP Top 10 Application Security Risks – 2017**: Es un documento que "se enfoca en identificar los riesgos de seguridad de aplicaciones web más serias para una amplia gama de organizaciones" (OWASP). Para cada uno de los riesgos identificados, dicha guía proporciona información sobre la probabilidad y el impacto basado en la Metodología de calificación de riesgo de OWASP, y una serie de consejos y buenas prácticas sobre cómo provenirlo.

Además de los tips y consejos que ofrece OWASP, se toman en cuenta las buenas prácticas que se contemplan en la página web de Yii2, el cual es el *framework* de PHP con el que se trabaja para el desarrollo del proyecto, y que cuenta con algunas bondades en cuanto a elementos de seguridad para el desarrollo de aplicaciones web.

Unos de los objetivos del proyecto es desarrollar una aplicación web que sea segura; en este sentido, el uso de la firma digital como una forma de autenticación es de suma importancia. Para lograrlo se requiere **investigar cómo trabaja el proceso de autenticación de usuarios en un sistema web mediante el uso de firma digital, con el objetivo de fortalecer el nivel de seguridad en la autenticación de los usuarios de la herramienta**.

Unas de las principales fuentes de información sobre el uso de firma digital en Costa Rica son la página web del Sistema Nacional de Certificación Digital (https://www.firmadigital.go.cr/verificacion/Verificacion.aspx), y la página web del Banco Central de Costa Rica (https://www.bccr.fi.cr/seccion-firma-digital/firma-digital); sin embargo, dentro de estas no se especifica de qué forma se podría

emplear la firma digital como mecanismo de autenticación para incrementar la seguridad en una aplicación, y para tal propósito deben quedar claros algunos aspectos como:

- Datos contenidos en el certificado de firma digital
- Formato de los datos del certificado de firma digital
- Mecanismo para obtener datos del certificado de firma digital
- Mecanismo para pasar información del certificado de firma digital a la aplicación web
- Validaciones para determinar vigencia del certificado de firma digital

Con el fin de amarrar todos los aspectos de los objetivos anteriormente descritos, se debe **elaborar la arquitectura de la solución para la automatización del modelo de madurez en ciberseguridad ECM2 que refleje el uso de estándares de seguridad estudiados durante la Maestría en Ciberseguridad**. Esta arquitectura debe mostrar la solución mediante la cual interactúa el usuario final; tanto externo como administrador del sitio, la aplicación web, servidor de aplicación, y servidor de base de datos, de forma tal que se ofrezca una estructura sólida que garantice que una aplicación funcional y segura.

El siguiente paso es **desarrollar una aplicación web segura que permita aplicar el modelo de madurez en ciberseguridad ECM2 en diferentes organizaciones sin importar su tamaño y sector**. Este punto contempla una serie de etapas y entregables que son indispensables para el adecuado desarrollo y documentación de un proyecto de desarrollo, para este caso específico se contemplan:

- Casos de uso
- Diagramas de secuencia
- Diagrama de base de datos (Entidad relación)
- Diccionario de datos
- Manual de usuario

- Código fuente de la aplicación

Durante la elaboración de estos entregables se debe tomar en cuenta que se tienen que **aplicar las mejores prácticas de seguridad en aplicaciones, servidores y bases de datos identificadas, con el fin de elaborar una herramienta de evaluación del nivel de seguridad que cumpla con medidas de seguridad, estudiados durante la Maestría en Ciberseguridad**. Como se ha venido recalcando, la idea es desarrollar una aplicación web que permita evaluar el estado de la Ciberseguridad en cualquier tipo de organización, y que dicha aplicación sea elaborada contemplando buenas prácticas para el desarrollo de aplicaciones seguras.

Por último, es importante **realizar pruebas funcionales y de seguridad de la aplicación, que permitan determinar si esta cumple con los requerimientos para la evaluación del nivel de seguridad de las instituciones, así como las mejores prácticas en materia de seguridad para el desarrollo de aplicaciones seguras**.

Para este objetivo se contemplan dos mecanismos de evaluación, uno manual y el otro automatizado. El primero de ellos mediante el uso de todas y cada una de las funcionalidades de la aplicación por medio de un usuario administrador y otro para usuarios externos, en primera instancia por parte de los estudiantes durante el proceso de desarrollo, posteriormente una demostración funcional al creador del modelo de madurez en ciberseguridad, Ingeniero Msc. César Rodríguez, y por último con un miembro del personal de CSIRT-CR. La segunda es mediante el uso de un software especializado en la realización de diferentes pruebas de penetración y seguridad de aplicaciones, en este caso el elegido es The OWASP ZedAttack Proxy (ZAP).

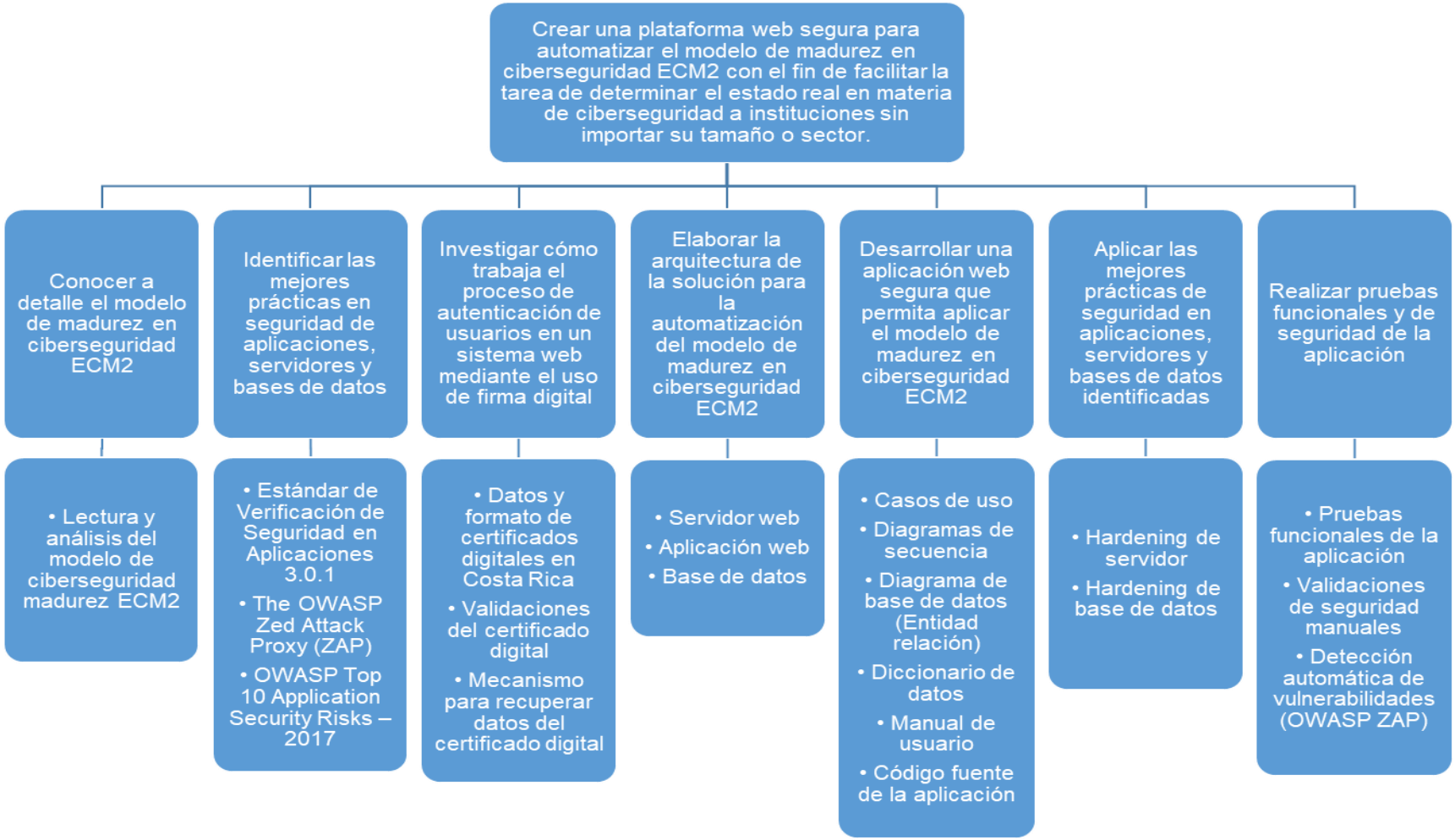


Ilustración 1 Diagrama EDT de la solución

Capítulo 5. Implementación de la solución y resultados

En este capítulo se presentan los resultados obtenidos durante el desarrollo de cada una de las actividades contempladas en la propuesta de solución para cada objetivo planteado. De la misma forma que en el capítulo anterior, los resultados se muestran en el orden en que se redactaron los objetivos.

El modelo de madurez en ciberseguridad ECM2 se compone de una lista de 14 dominios, los cuales agrupan un total de 63 controles de seguridad a evaluar. “Cada control constituye un área en particular a evaluar en el tema de la Ciberseguridad, mientras que los dominios pretenden organizar estos controles de manera que la implementación del modelo sea más ordenada” (Rodríguez Bravo, 2017).

La evaluación de cada control se hace con una escala de 5 niveles, que van desde el nivel 0; el más bajo que indica la inexistencia del control, hasta el nivel 4; el más alto y que refleja un nivel de madurez muy alto que incluso es reconocido por otras entidades. El nivel1 indica que se está en proceso de creación de controles, pero no se han implementado, el nivel 2 refleja la existencia de controles, pero se podrían estar aplicando de forma incorrecta, y el nivel 3 que significa la existencia de controles y se implementan de forma correcta.

Para interpretar los resultados, se parte del supuesto que “la fortaleza de una cadena es equivalente al más débil de sus eslabones”. Por lo tanto, la calificación será el nivel más bajo obtenido de todos los controles evaluados aplicables, ya sea por dominio o a nivel de empresa en general.

La manera en que se deben interpretar los resultados de la aplicación del modelo de madurez en Ciberseguridad ECM2, el detalle de todos los dominios, y sus respectivos controles, así como la descripción de cada uno de los niveles de dicho modelo, se encuentran en la tesis de Maestría en Ciberseguridad del Ingeniero Máster César Rodríguez Bravo (Rodríguez Bravo, 2017).

Como parte de la tarea de identificar las mejores prácticas en seguridad de aplicaciones, servidores y bases de datos, con el fin de desarrollar una aplicación web que permita la evaluación del nivel de ciberseguridad en diversas organizaciones y cumpla con estándares en la materia, se trató de incorporar la mayor cantidad posible de consejos y buenas prácticas tanto del Estándar de verificación de seguridad en aplicaciones 3.0.1, así como del Top 10 Application security risk.

Entre las mejores prácticas del Top 10 Application security risk se pueden destacar:

Riesgos de seguridad	Cómo prevenir
Inyección	• Para cualquier consulta dinámica residual, escape caracteres especiales utilizando la sintaxis de caracteres.
Pérdida de autenticación y gestión	• Implementar autenticación multifactor. • Utilizar una política de longitud, complejidad y rotación de contraseñas. • Limitar o incrementar el tiempo de respuesta de cada intento fallido de inicio de sesión. • Registrar todos los fallos. • Utilizar un gestor de sesión en el servidor, integrado, seguro y que genere un nuevo ID de sesión aleatorio con alta entropía después del inicio de sesión. • El Session-ID no debe incluirse en la URL.
Exposición de datos sensibles	• No almacenar datos sensibles innecesariamente. • Cifrar todos los datos sensibles cuando sean almacenados. • Utilizar únicamente algoritmos y protocolos estándares y fuertes e implementar una gestión

	adecuada de claves. • No crear algoritmos de cifrado propios. • Almacenar contraseñas utilizando funciones de *hashing*.
Pérdida de control de acceso	• Con la excepción de los recursos públicos, la política debe ser denegar de forma predeterminada. • Implementar los mecanismos de control de acceso y reutilizarlo en toda la aplicación. • Deshabilitar el listado de directorios del servidor web. • Los *tokens* deben ser invalidados luego de la finalización de la sesión por parte del usuario.
Configuración de seguridad incorrecta	• Usar una plataforma minimalista sin funcionalidades innecesarias, componentes, documentación o ejemplos. • Eliminar o no instalar *frameworks* y funcionalidades no utilizadas. • La aplicación debe tener una arquitectura segmentada que proporcione una separación efectiva y segura entre componentes y acceso a terceros.
Secuencia de comandos en sitios cruzados (XSS)	• Codificar los datos de requerimientos HTTP no confiables en los campos de salida HTML (cuerpo, atributos, Java Script, CSS, o URL).

Uso de componentes con vulnerabilidades conocidas	• Remover dependencias, funcionalidades, componentes, archivos y documentación innecesaria y no utilizada. • Supervisar bibliotecas y componentes que no poseen mantenimiento o no liberan parches de seguridad para sus versiones obsoletas o sin soporte
Registro y monitoreo insuficientes	• Registrar fallos en inicio de sesión de usuarios administradores

Tabla1Resumen OWASP Top 10 Application Security Risks – 2017

Además, está el Estándar de Verificación de Seguridad en Aplicaciones 3.0.1, cabe destacar que, con el propósito de construir una solución segura, muchos de los elementos presentes en las listas de verificación pasaron a ser requerimientos no funcionales entre los cuales destacan los siguientes:

Dominio	Se identifica que
Arquitectura, diseño y modelado de amenazas	• No exista ninguna lógica de negocio con datos sensibles, como claves secretas o información sensible del lado del cliente. • Los componentes presentes en la aplicación sean solo los necesarios para su funcionamiento. • Los componentes que conforman la solución no cuenten con vulnerabilidades conocidas.
Verificación de autenticación	• Las páginas y recursos requieran autenticación, salvo las que son de orientadas a ser públicas. • Los controles de autenticación se realicen del lado del servidor. • Las credenciales de autenticación para acceder se

	encuentran cifradas en la base de datos. • La aplicación previene los ataques de fuerza bruta automatizados bloqueando, inhabilitando el usuario luego de varios intentos. • Las rutas de recuperación de contraseñas expiran después de cierto tiempo y solo se permite usarlas una vez. • Se implementa la funcionalidad de solicitar la contraseña anterior para el cambio de contraseña, además de que es requerido confirmar la nueva contraseña. • Los usuarios se bloquean por un tiempo prudencial después de varios intentos fallidos de inicio de sesión.
Gestión de sesiones	• Las sesiones se invalidan cuando el usuario cierra sesión. • Las sesiones se invalidan después de un cierto tiempo de inactividad.
Control de acceso	• Se parte del principio de privilegio mínimo donde el usuario solo tiene autorización de realizar ciertas funciones. • Se deshabilita la navegación entre directorios.
Manejo de entrada de datos	• Se validan las rutinas de entrada del lado del servidor • Se verifica que los controles no sean susceptibles a desbordamientos de *buffer*. • Se validan los controles según tipos de datos • Se manejan estructuras de datos fuertemente tipados • Se aseguran que el manejo de *strings* sea llevado apropiadamente de manera que no sean susceptibles a manipulaciones del DOM, o Site

	Scripting (XSS).
configuración de seguridad HTTP	• Cada cabecera específica el *content-type* donde se especifica el conjunto de caracteres seguros

Tabla 2 Resumen Estándar de Verificación de Seguridad en Aplicaciones 3.0.1

Como siguiente paso en el desarrollo del proyecto, se planteó investigar cómo trabaja el proceso de autenticación de usuarios en un sistema web mediante el uso de firma digital, con el objetivo de fortalecer el nivel de seguridad en la autenticación de los usuarios de la herramienta. Por lo que se detallan los principales aspectos a considerados para este objetivo:

Datos contenidos en el certificado de firma digital: Lo más relevante en este punto es identificar la información personal del usuario en el certificado, la cual va a ser utilizada para la autenticación en la aplicación web. Esta información se encuentra en el campo Asunto (Subject) del certificado:

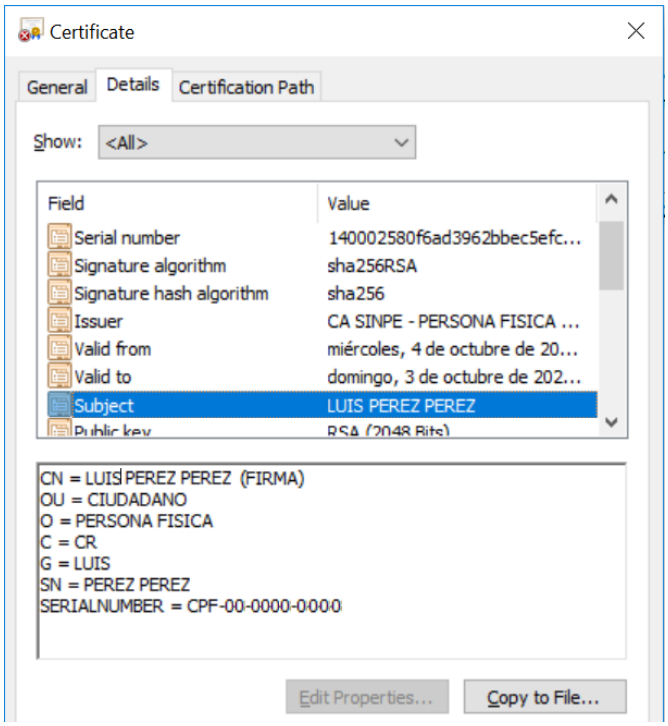


Ilustración 2 Detalle del Subject en el certificado digital

Formato de los datos del certificado de firma digital:

Atributo	*Valor*	*Descripción*
Country (C)	CR	El código de país es asignado de acuerdo al estándar ISO 3166
Organization (O)	PERSONA FISICA	La política identifica si se trata de un certificado para: Persona Física, Persona Jurídica o Sellado de Tiempo, o bien otra definida por la jerarquía nacional de certificadores registrados.
Organization Unit (OU)	CIUDADANO	La clase de certificado es: CIUDADANO, EXTRANJERO o DIPLOMÁTICO.
Common Name	JUAN PEREZ (FIRMA)	Nombre del suscriptor, según documento de identificación oficial, en mayúsculas y sin tildes El propósito debe ser FIRMA o AUTENTICACIÓN.
Serial Number {OID:2.5.4.5}	CPF-01-0449-0161	El formato del documento de identificación se especifica en la sección 3.1.4 “Reglas para la interpretación de varias formas de nombres”.
Surname (SN) {OID:2.5.4.4}	PEREZ PEREZ	Se registran los dos apellidos del suscriptor, en mayúsculas y sin tildes.
GivenName (G) {OID:2.5.4.42}	JUAN	Se registra el nombre del suscriptor, en mayúsculas y sin tildes.

Tabla 3 Formato de información personal del certificado digital

Mecanismo para obtener datos del certificado de firma digital, y Mecanismo para pasar información del certificado de firma digital a la aplicación web

Estos dos puntos se abordaron de manera simultánea, y bajo la misma solución, ya que durante el proceso de investigación sobre el uso de firma digital como medio de autenticación para sitios web, se identificó un aplicativo realizado por parte de RACSA para el Sistema Integrado de compras públicas en Costa Rica (SICOP), llamado Componente Firma, el cual consiste en un API que realiza la comunicación entre los lectores de tarjetas inteligentes y los navegadores web.

Con el fin de aprovechar la funcionalidad de este aplicativo se contactó con personal de dicho proyecto en RACSA y se obtuvo una carta de autorización por parte de los mismos para el estudio y utilización de este con fines educativos y que no sean de lucro; ver Anexo 4: Carta autorización Racsa.

Como se mencionó anteriormente, esta aplicación tiene la capacidad de leer la información de la tarjeta de firma digital, y pasarla a un navegador web, por lo que se trabajó en determinar exactamente cuál información se lee, en qué formato, y cómo utilizarla para el proceso de autenticación.

Validaciones para determinar vigencia del certificado de firma digital

Dentro del certificado existen un par de campos destinados para la vigencia del certificado, uno con la fecha de inicio de validez y el otro con la fecha fin de validez:

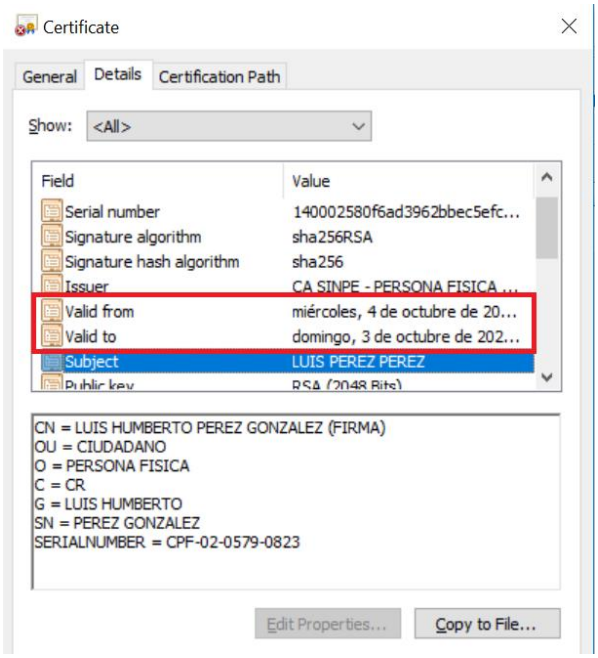


Ilustración 3 Vigencia del certificado digital

Para la elaboración de la arquitectura, se tomaron en cuenta dos factores, que la propuesta estuviera alineada con las plataformas y conocimiento del personal del CSIRT-CR, con el fin de que estos puedan brindar mantenimiento e incorporar mejoras en el futuro, y que los elementos por incluir en la propuesta, fueran los idóneos para el abordaje del problema y de la solución.

Con tales elementos en mente se buscó completar el objetivo de **elaborar la arquitectura de la solución para la automatización del modelo de madurez en ciberseguridad ECM2 que refleje el uso de estándares de seguridad estudiados durante la Maestría**.

Como resultado se plantea la siguiente propuesta:

Un modelo cliente servidor con tecnologías de código abierto, en donde el cliente tenga la posibilidad de realizar la autenticación por medio de su certificado firma digital, logrando con esto evitar problemas de *phishing, keylogging*, además de evitar el inconveniente que muchas veces conlleva el recordar múltiples credenciales.

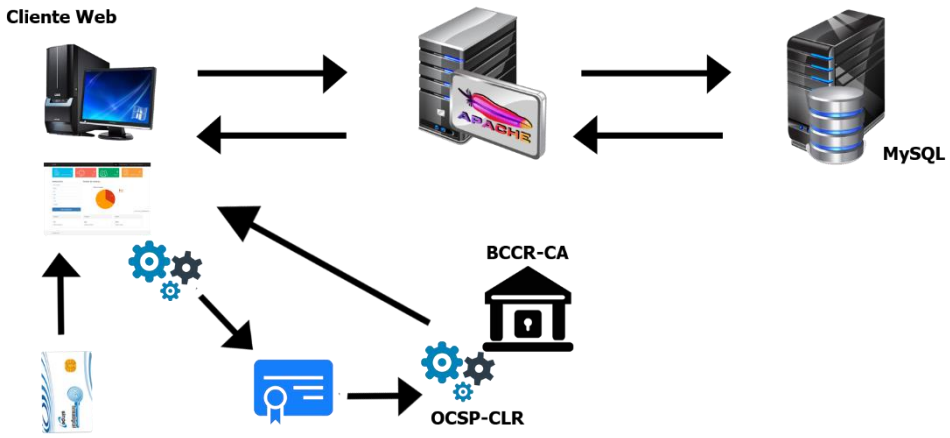


Ilustración 4 Arquitectura de la aplicación

En la arquitectura la dinámica de la aplicación funciona de la siguiente manera:

Opción firma digital

- El usuario ingresa a la aplicación, seleccionando el método de autenticación, por medio del certificado de digital.
- El sitio web solicita el certificado.
- El usuario ingresa la tarjeta de firma al dispositivo lector.
- La aplicación web reconoce el certificado, y solicita el ingreso del PIN.
- El usuario ingresa el PIN y la aplicación inicia el proceso de validación el cual consiste en los siguiente:
    - La aplicación lee el certificado y realiza la comprobación que este pertenezca a la raíz nacional.
    - Que las fechas de validez incluida en los atributos del certificado se encuentren vigentes.
    - Que el certificado no se encuentre incluido en la lista de revocación.
    - Que el estado del certificado en el servicio OCSP sea válido.

- Una vez que las comprobaciones anteriores sean realizadas, se valida que el usuario se encuentre inscrito en la aplicación, y que este tenga como método de inicio de sesión designado el uso de certificado.
- El usuario ingresa a la aplicación.

Opción usuario y contraseña

- El usuario ingresa a la aplicación, selecciona como método de autenticación la opción de usuario y contraseña.
- El usuario digita sus credenciales y presiona el Iniciar sesión.
- Si las credenciales son correctas, el usuario ingresa a la aplicación.

Una vez dentro de la aplicación, independientemente de la opción de autenticación, el usuario puede interactuar con la interfaz de acuerdo con su perfil.

Es importante recordar que la aplicación cuenta con dos perfiles primarios en donde existe un usuario administrador el cual tiene la posibilidad de alimentar, consultar y modificar los diferentes mantenimientos que conforman la aplicación, así como las evaluaciones realizadas por los usuarios, independientemente de la institución.

Para el perfil de administrador, la aplicación presenta al usuario un panel de administración con algunos accesos directos a los mantenimientos, así como alguna información relevante sobre los mismos. Para mayores detalles, se recomienda visitar el manual de usuario incluido en los anexos.

Para el perfil de usuario externo, se crea una interfaz en donde este tiene la posibilidad de autogestionar la creación de sedes, para la institución, así como el crear consultar y modificar evaluaciones, además de tener la posibilidad de ver esta información en forma de gráficos. Para ello, nuevamente se recomienda ver el manual de usuario incluido en el documento.

Una vez definida la arquitectura sobre la cual se debe trabajar, inicia el proceso para cumplir con el objetivo de **desarrollar una aplicación web segura que**

permita aplicar el modelo de madurez en ciberseguridad ECM2 en diferentes organizaciones sin importar su tamaño y sector.

Casos de uso:

> Un caso de uso es una descripción de las acciones de un sistema desde el punto de vista del usuario. Es una herramienta valiosa dado que es una técnica de aciertos y errores para obtener los requerimientos del sistema, justamente desde el punto de vista del usuario (Cevallos, UML: Casos de Uso, 2015).

Los casos de uso describen la interacción, acciones o mensajes, que se dan entre una aplicación y el usuario o usuarios de esta, sin hacer uso de lenguaje muy técnico, sino más bien simple y fácil de entender. Generalmente se realiza un caso de uso por cada una de las funcionalidades del sistema. Los casos de uso de la aplicación para llevar a cabo la automatización del modelo de madurez en Ciberseguridad ECM2 están en el Anexo 1: Caso de uso.

Diagramas de secuencia:

> Un diagrama de secuencias muestra la interacción de un conjunto de objetos de una aplicación a través del tiempo, en el cual se indicarán los módulos o clases que formaran parte del programa y las llamadas que se hacen cada uno de ellos para realizar una tarea determinada, por esta razón permite observar la perspectiva cronológica de las interacciones (Cevallos, 2015).

Generalmente los diagramas de secuencia se asocian a un caso de uso o funcionalidad del sistema; a continuación, se presentan los diagramas de secuencia más relevantes de la aplicación web para la automatización del modelo de madurez en Ciberseguridad ECM2:

Para ingresar al sistema el usuario cuenta con dos formas de autenticación, una mediante el uso de usuario y contraseña, y la otra mediante firma digital, la cual es más recomendable.

El proceso de **autenticación por usuario y contraseña** es el más común, y consiste en que este digite su id y contraseña, y la aplicación debe realizar una comparación con las credenciales de la base de datos; en caso de ser exitoso, permite el ingreso; en caso contrario, lo deniega y además, guarda un registro en la base de datos con el intento de ingreso fallido y al contabilizar 4 intentos fallidos consecutivos, bloquea temporalmente el usuario, impidiendo su ingreso al sistema, esto como medida de seguridad.

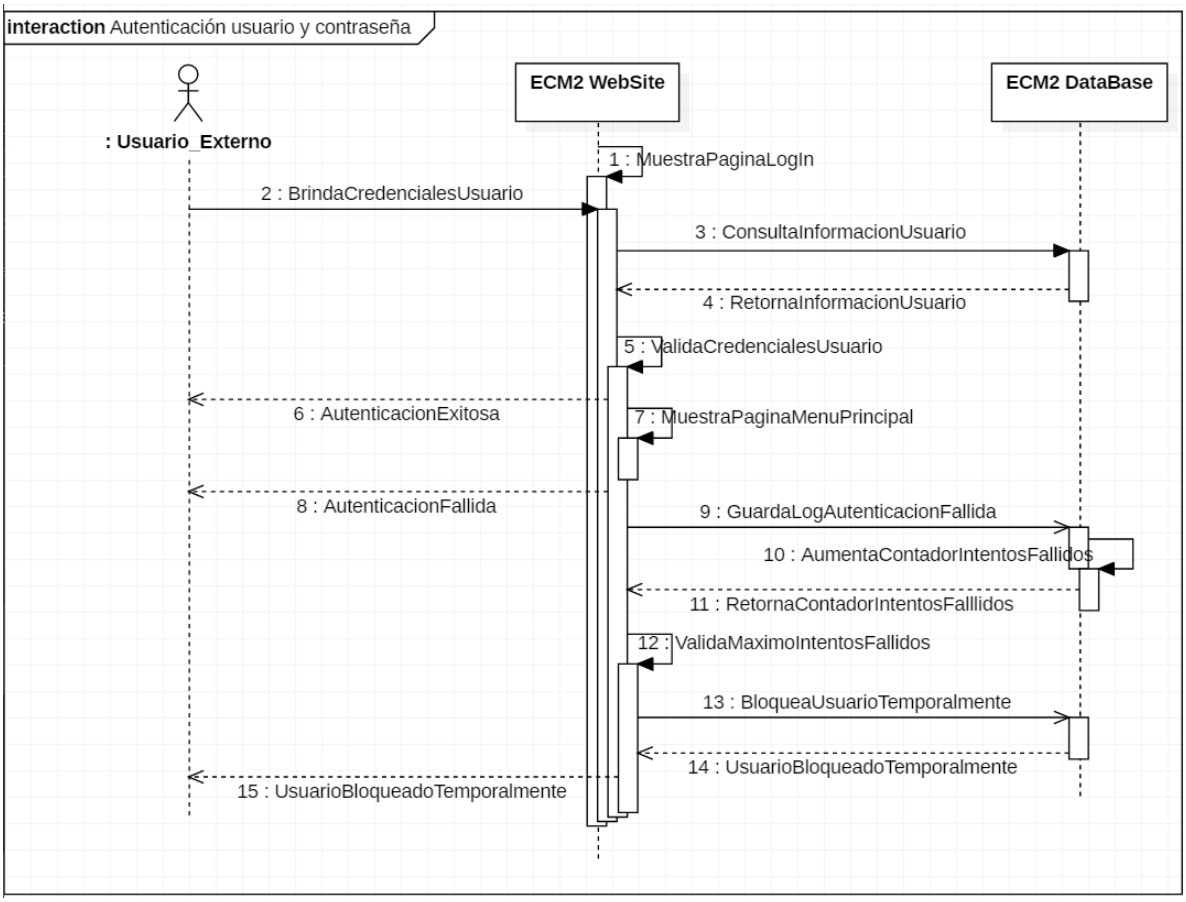


Ilustración 5 Diagrama Autenticación usuario y contraseña

Para la **autenticación por medio de firma digital**, el usuario debe tener instalado el Componente de Firma, desarrollado por RACSA; al momento de ingresar al sistema, debe seleccionar la opción de autenticación por firma digital, el componente lee los datos de la tarjeta, los envía al navegador (sistema web), este solicita el PIN del certificado; si el PIN es correcto, el Componente de Firma procede a verificar que esté vigente y que no se encuentre revocado.

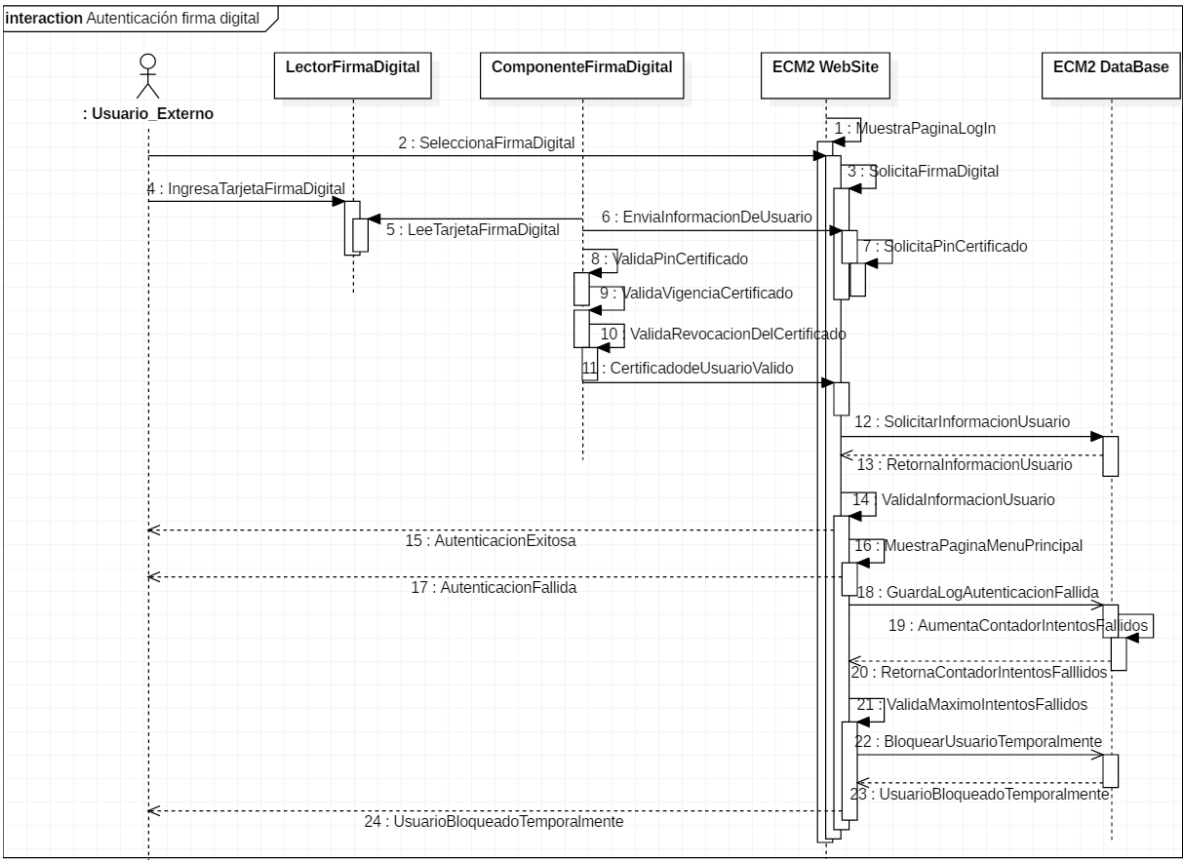


Ilustración 6 Diagrama autenticación con firma digital

Una vez que el usuario ha sido autenticado, puede proceder a crear y consultar evaluaciones:

Para crear evaluaciones, el usuario se dirige al menú de evaluaciones, el sistema muestra una lista de las que han sido creadas, y un botón para crear una nueva evaluación. Cuando se procede a crearla, el sistema muestra una página en la

cual solicita al usuario que seleccione la sede de su compañía en la que desea aplicar la evaluación y que digite una descripción para identificarla.

Una vez que la evaluación ha sido creada, el sistema muestra la lista de dominios que contempla el modelo de madurez en Ciberseguridad ECM2, y para cada uno de ellos habilita la opción de “Evaluar”, y si el usuario ingresa a dicha evaluación se listará los diferentes controles y sus respectivos niveles para calificar, así como un campo de texto en el que el usuario puede realizar observaciones.

A medida que el usuario ha evaluado controles y dominios, se va reflejando la calificación o nivel de madurez obtenido, el cual como ya se mencionó, corresponde al valor del mínimo nivel obtenido.

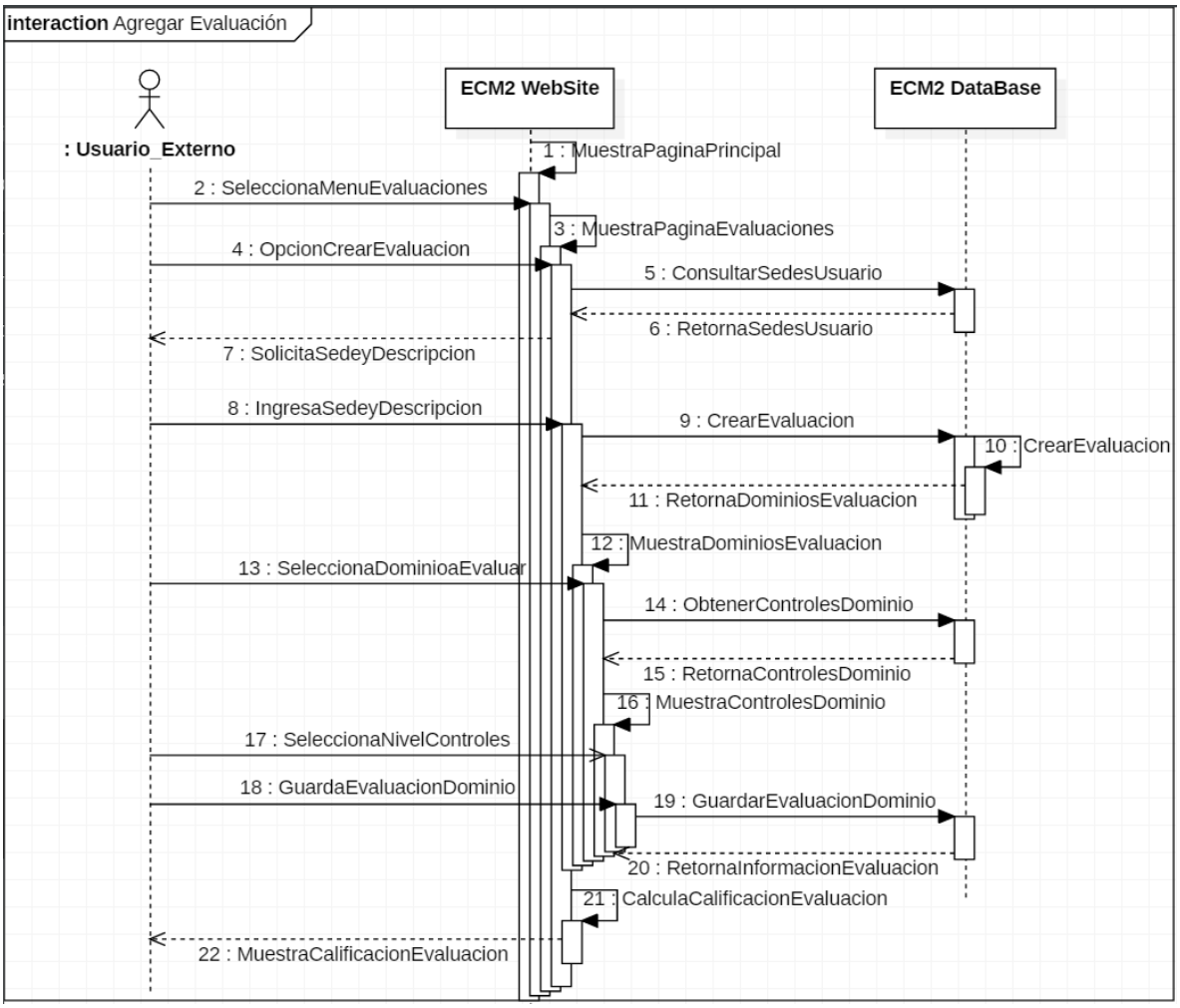


Ilustración 7 Diagrama agregar evaluación

Si lo que desea el usuario es consultar o completar/modificar una evaluación, debe presionar la opción “Ver detalles” de evaluación que desea consultar, y posteriormente, el sistema muestra la lista de dominios con su respectiva calificación y habilitada para su edición.

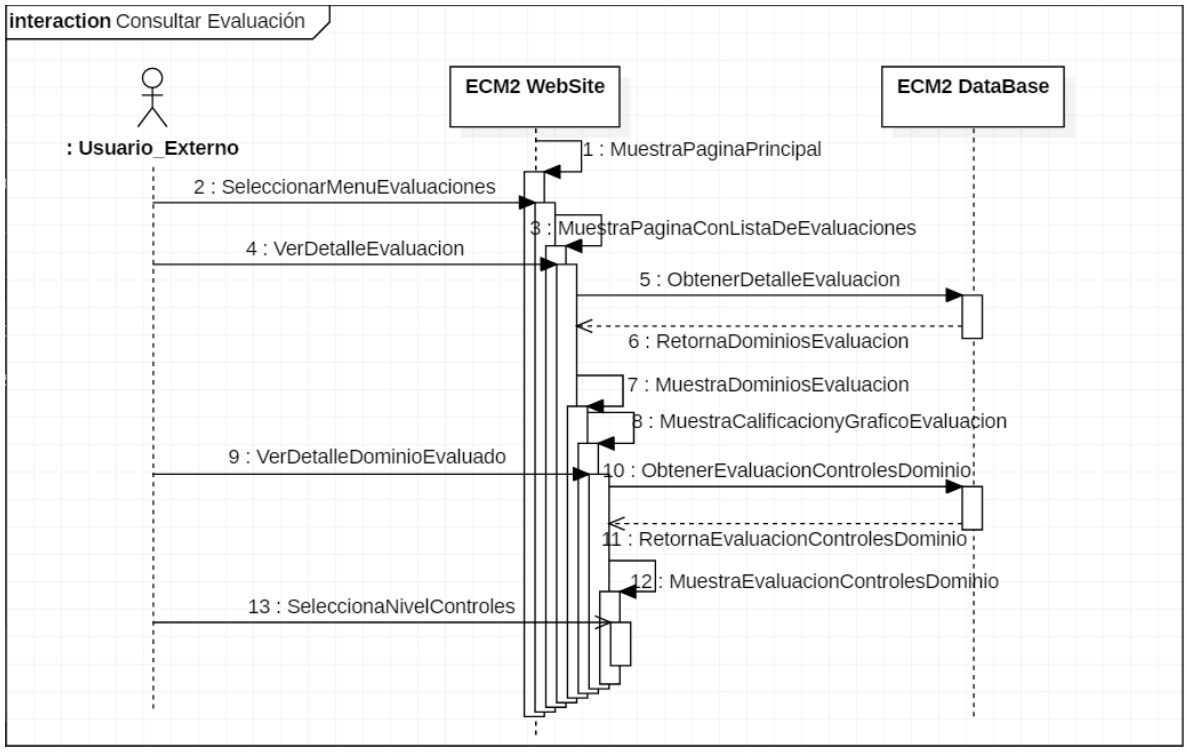


Ilustración 8 Diagrama consultar evaluación

Los mantenimientos del sistema están del lado del Administrador y de estos, la creación; además la opción de activar/inactivar usuarios tiene particularidades y por ello se detallan a continuación.

En el caso de creación de usuarios, el administrador ingresa a la opción de mantenimientos, dentro de esta debe seleccionar el mantenimiento de usuarios, y posteriormente el botón que le permite agregar uno nuevo. El administrador ingresa los datos del nuevo usuario y presiona la opción de crear, el sistema valida que no exista otro usuario con esa misma cédula y/o dirección de correo electrónico y posteriormente presiona el botón para crear el usuario, el cual se ingresa en estado “inactivo”.

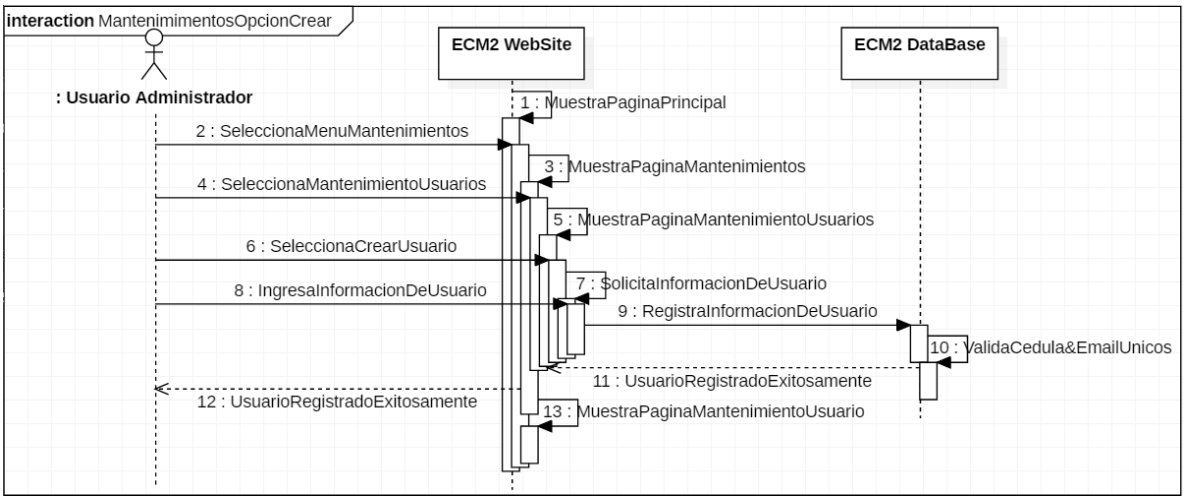


Ilustración 9 Mantenimiento agregar usuario

Una vez que el usuario ha sido creado, el administrador puede proceder a cambiar su estado para activarlo, con lo cual el sistema procede a generar un *token* temporal mediante el cual crea un URL que es enviado al correo electrónico del usuario, para que este proceda a ingresar y actualizar su contraseña. En caso de que el usuario esté activo y el administrador quiera inactivarlo, el sistema realiza actualización del estado en la base de datos, pero no notifica al usuario.

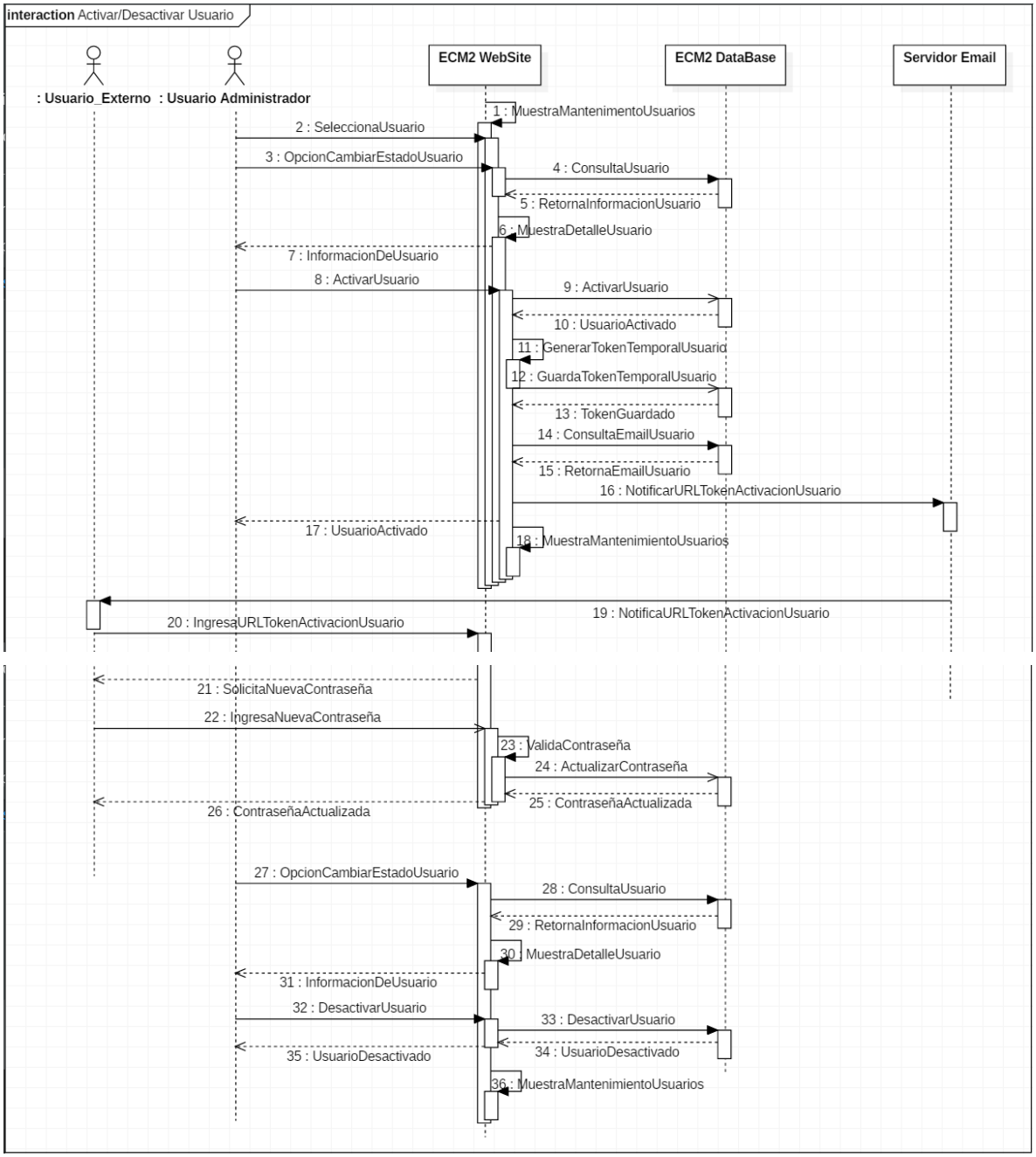


Ilustración 10Diagrama activar/desactivar usuario

Modelo de base de datos

Una vez identificados los principales requerimientos y funcionalidades del sistema, se procedió con la creación del modelo entidad relación de la base de datos. Dentro de las principales consideraciones se contempló:

- La posibilidad de que el modelo de madurez en ciberseguridad ECM2 pueda sufrir modificaciones y se agreguen o eliminen dominios, controles y/o niveles.
- Que una institución pueda tener más de una sede, y que cada una de ellas se evalúe de forma separada.
- Que una institución pueda tener más de un encargado de realizar evaluaciones.
- Que se pueda realizar más de una evaluación por institución/sede, y que estas se registren por fecha, y contemplando un consecutivo a nivel de sede.
- Que se guarde un registro de los intentos de sesión fallidos por usuario.
- Que se contemple el manejo de roles de usuarios para el ingreso al sistema.

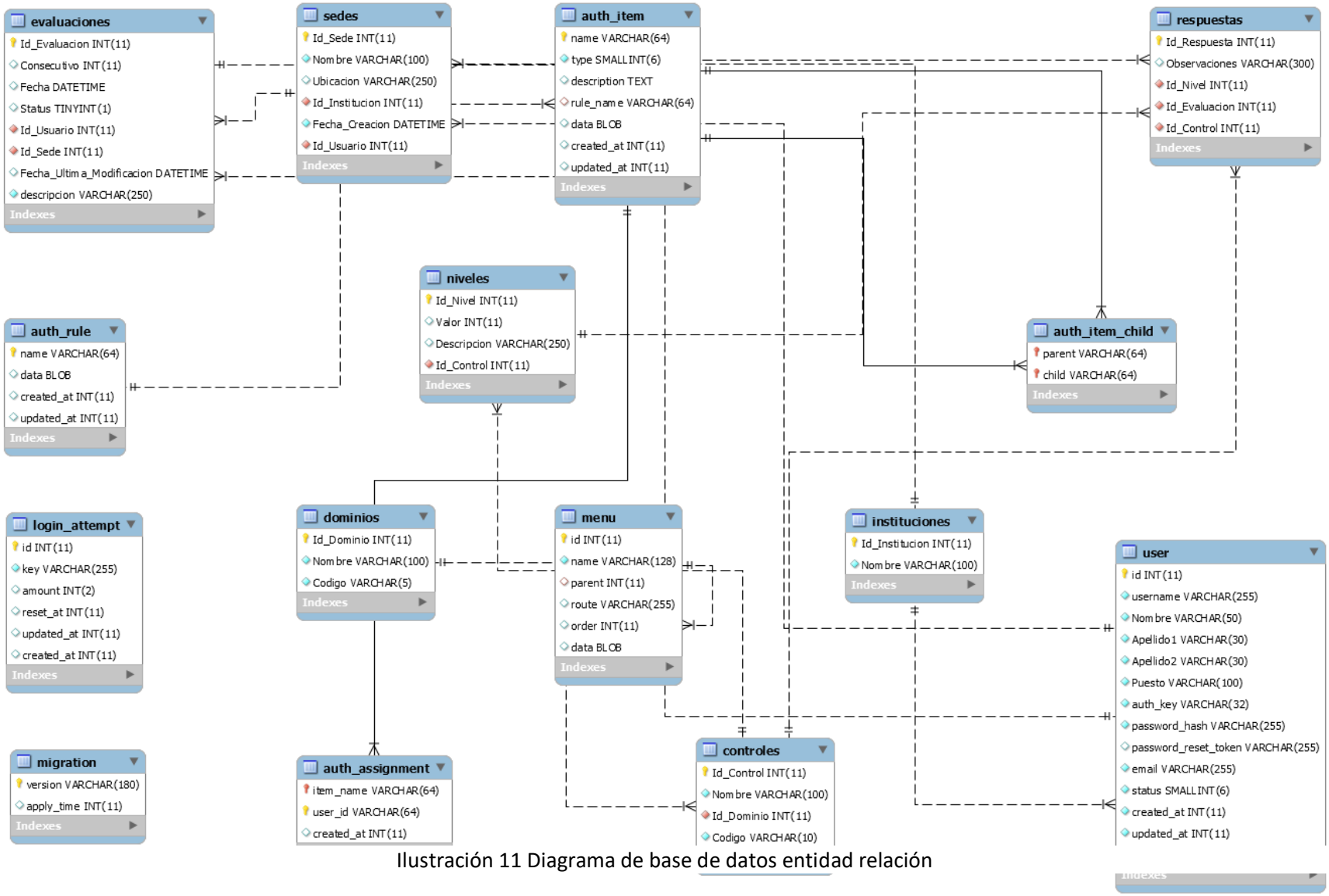


Ilustración 11 Diagrama de base de datos entidad relación

Diccionario de datos

Refiriéndose a un diccionario de datos, Codina (1998) indica que “consiste en la lista detallada de cada uno de los campos que forman los distintos modelos de registro de la base de datos”. Además, indica que por cada uno de los campos se debe contemplar al menos los siguientes aspectos:

- Etiqueta (Nombre del campo)
- Dominio (Descripción)
- Tipo de datos
- Indexación
- Controles de validación (¿Permite nulos?)
- Ejemplos válidos

El diccionario de datos puede verse como una descripción detallada del modelo de base de datos, en el cual se incluyen las tablas del modelo, y por cada una de estos la especificación de los campos. En el Anexo 2: Diccionario de datos, se encuentra este detalle de la base de datos utilizada en la aplicación para la automatización del modelo de madurez en ciberseguridad ECM2.

Manual de usuario

Para Porto &Gardey (2013), el manual de usuario “se trata de una guía que ayuda a entender el funcionamiento de algo”; además indican que “es un documento de comunicación técnica, que busca brindar asistencia” a los usuarios de la

aplicación. En el manual de usuario se detalla el paso a paso de cada una de las funciones de la aplicación, sus restricciones y los responsables de realizarlas.

El documento adjunto en el Anexo 3: Manual de usuario, permite a los usuarios entender la forma en que se debe manejar la aplicación, y explica punto por punto la distribución de los menús y los ítems que puede encontrar en estos, así como los requisitos para operar los mantenimientos y la explicación de cómo agregar nuevos permisos o removerlos, además el cómo interpretar los gráficos, entre otros.

Los dos últimos objetivos del proyecto están estrechamente relacionados; el primero de ellos: **aplicar las mejores prácticas de seguridad en aplicaciones, servidores y bases de datos identificadas, con el fin de elaborar una herramienta de evaluación del nivel de seguridad que cumpla con medidas de seguridad estudiados durante la Maestría en Ciberseguridad**, y el segundo: **realizar pruebas funcionales y de seguridad de la aplicación, que permitan determinar si esta cumple con los requerimientos para la evaluación del nivel de seguridad de las instituciones , así como las mejores prácticas en materia de seguridad para el desarrollo de aplicaciones seguras**.

Para cumplir con el primero de los dos objetivos citados anteriormente, se puso en práctica la mayor cantidad posible de buenas acciones que se identificaron durante la etapa inicial del proyecto; las cuales ya fueron detalladas en esta sección de resultados del documento.

Una vez que se analizaron los documentos OWASP Top 10 Application Security Risks – 2017, y Estándar de Verificación de Seguridad en Aplicaciones 3.0.1, y se hizo un resumen de las prácticas que se consideraron más relevantes para el proyecto, se procedió a tomarlas en cuenta durante la etapa de codificación y desarrollo de la aplicación para demostrar

con resultados que la aplicación cuenta con un nivel aceptable en el apartado de seguridad; para el último de los objetivos del proyecto, lo más conveniente y objetivo fue realizar un test o prueba automatizada que efectuara un escaneo de vulnerabilidades y con base en los resultados de este, tomar las acciones correctivas correspondientes. Como ya se mencionó, la herramienta seleccionada con este propósito fue The OWASP ZedAttack Proxy (ZAP).

ZAP es una herramienta gratuita y muy popular para el escaneo de vulnerabilidades en aplicaciones web. Según detalla Velasco (2015), unas de las principales características de ZAP son:

- Totalmente gratuita y de código abierto.
- Multi-plataforma, compatible incluso con Raspberry Pi.
- Fácil de instalar, dependiendo únicamente de Java 1.7 o superior.
- Permite asignar un sistema de prioridades.
- Traducida a más de 12 idiomas, entre ellos, el español.
- Excelente manual de ayuda y gran comunidad en la red.

Asimismo, Velasco (2015) la describe como una “herramienta forense de seguridad”, cita entre sus principales funciones:

- Análisis automáticos.
- Análisis pasivos.
- Cuenta con un “modo de ataque” para buscar vulnerabilidades.
- Posibilidad de comprobar todas las peticiones y respuestas entre cliente y servidor.
- Posibilidad de localizar recursos en un servidor.
- Posibilidad de lanzar varios ataques a la vez.

- Capacidad para utilizar certificados SSL dinámicos.
- Soporte para utilizar tarjetas inteligentes (DNI-e, por ejemplo) y certificados personales.
- Análisis de sistemas de autenticación.
- Posibilidad de actualizar la herramienta automáticamente.
- Dispone de una tienda de extensiones (plugins) con las que añadir más funcionalidades a la herramienta.

A continuación se explica la forma en la que se realizó el test sobre del sitio web publicado localmente; http://yii2-starter.dev, y algunos de los resultados obtenidos, así como los ajustes que se debieron realizar:

La versión instalada es la 2.7.0, para el sistema operativo Windows, ya que es el ambiente que se configuró para el desarrollo:

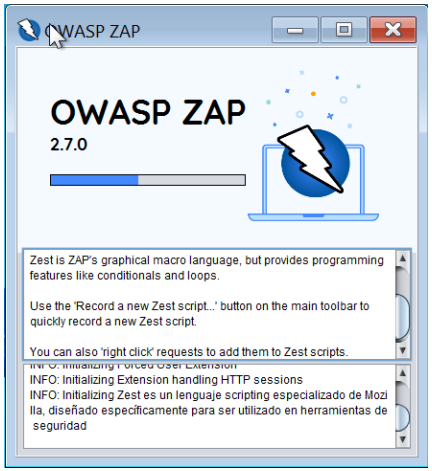


Ilustración 12 OWASP ZAP inicio

A continuación, se presenta la interfaz de usuario principal, en la cual se muestran el menú de opciones, así como un panel izquierdo en el cual se muestran las direcciones de los diferentes sitios a los que se les ha realizado el test, en panel derecho una bienvenida a la herramienta, así como un campo de texto para pegar la URL del sitio web al que se le quiera realizar un escaneo o test, y un botón con la opción “Atacar”, para iniciar las pruebas. En el panel inferior se muestran los resultados de los ataques o escaneo realizados, el detalle de las vulnerabilidades encontradas se muestra en la pestaña “Alertas”.

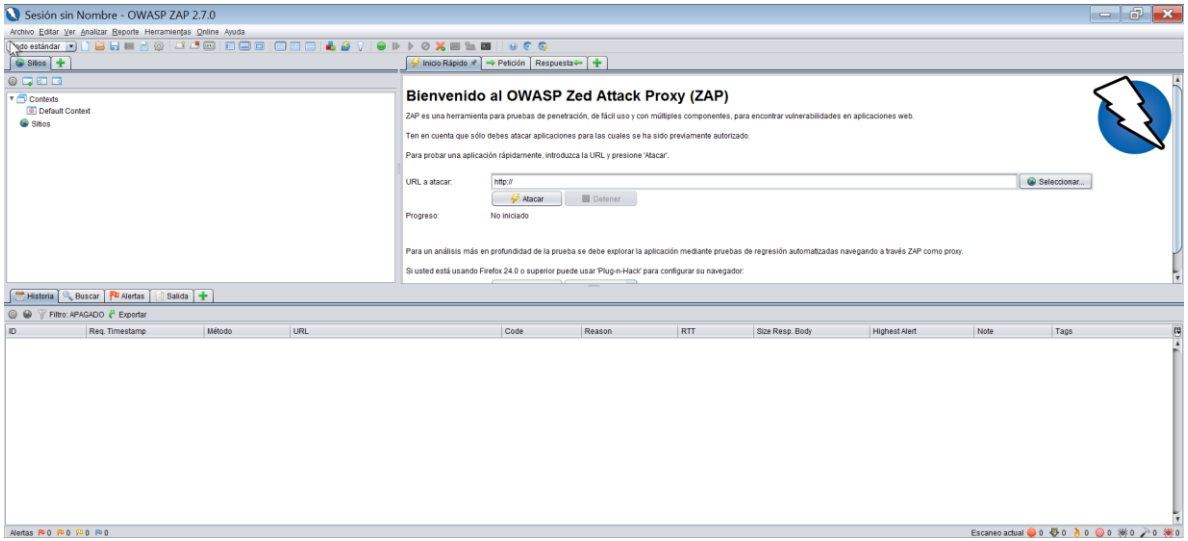
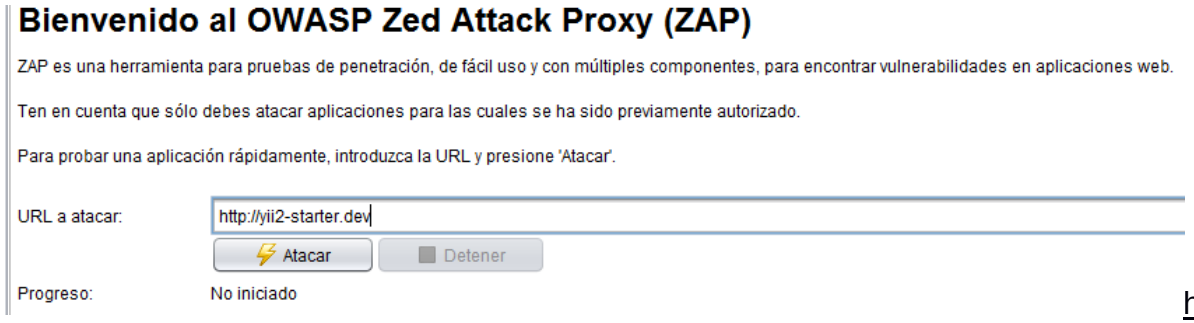


Ilustración 13 OWASP ZAP Principal

Para este caso, como se mencionó anteriormente, el sitio web corresponde a



http://yii2-starter.dev:

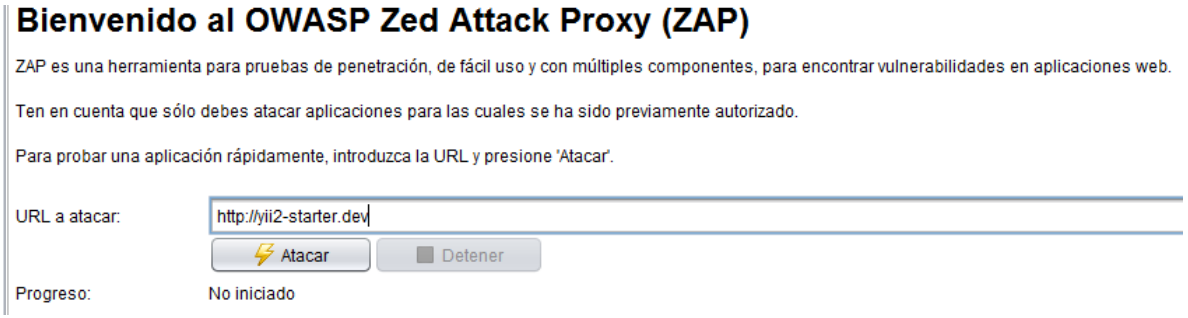


Ilustración 14OWASP ZAP Agregar URL

Los primeros resultados arrojados por la herramienta durante el escaneo indicaban que había alertas de riesgo “Low” o bajas, y se trataba de la ausencia de un atributo en los campos de texto para la contraseña en el *login* de usuarios, el cual no evita que de forma predeterminada haya un autocompletar de los campos de texto. Esto puede suponer un riesgo a la seguridad ya que si el autocompletar del navegador por defecto es verdadero, existe la posibilidad de que tanto el id de usuarios como contraseña sean recordadas en el navegador.

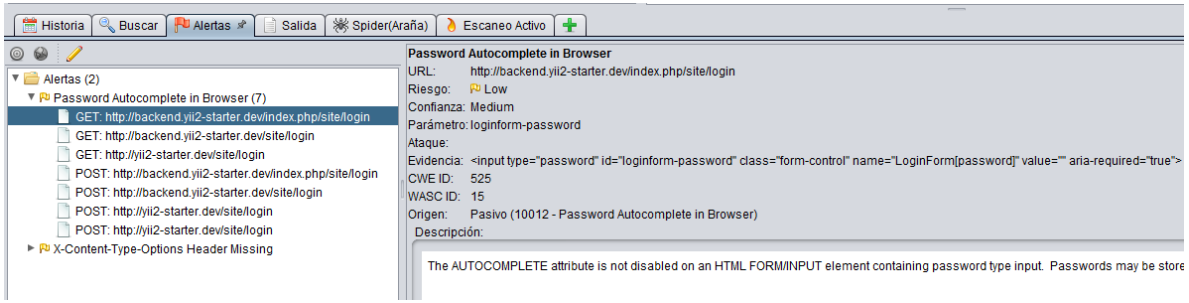


Ilustración 15 OWASP ZAP Resultado 1

Otra de las alertas encontradas por la aplicación indicaba que se podía ver el contenido de algunos directorios o carpetas que no eran precisamente contenido web, lo cual podría exponer recursos de la aplicación como *scripts*, archivos ocultos, imágenes, entre otros:

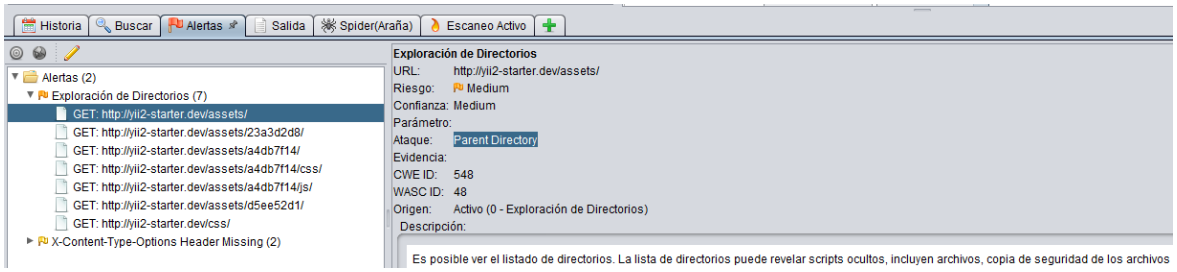


Ilustración 16 OWASP ZAP Resultado 2

Al realizar navegación por la ruta indicada en la herramienta, efectivamente se mostraban algunas carpetas con archivos de *logs* y algunos *scripts* de la aplicación, lo cual debió ser ajustado.

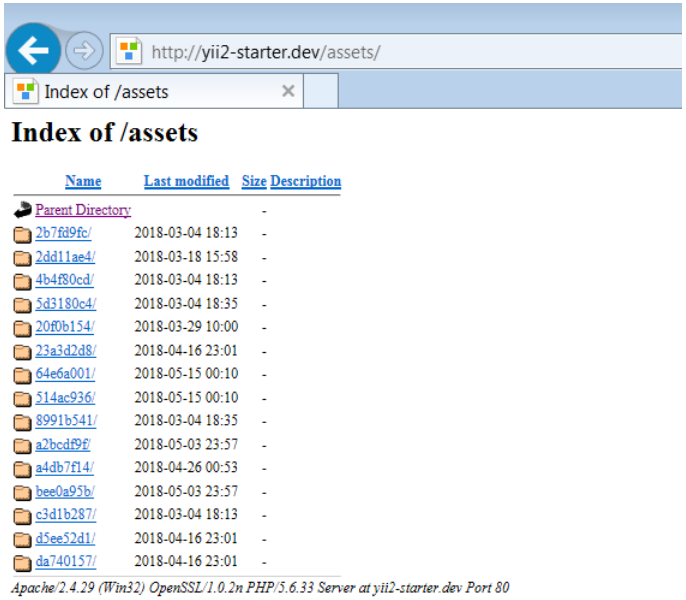


Ilustración 17 Navegación en directorios

Para este caso específico, se aplicó una modificación al archivo .htaccess, que se encuentra en el directorio raíz del proyecto, el cual consiste en agregar en la primera línea de dicho archivo la siguiente línea:

Options–Indexes

Luego de los ajustes solicitados por la herramienta, se logró eliminar las alertas para el último ataque realizado; 4963 registros de ataques o diferentes pruebas automáticas en dicho ataque, con lo cual se obtuvo el mejor resultado esperando en esta evaluación de seguridad:

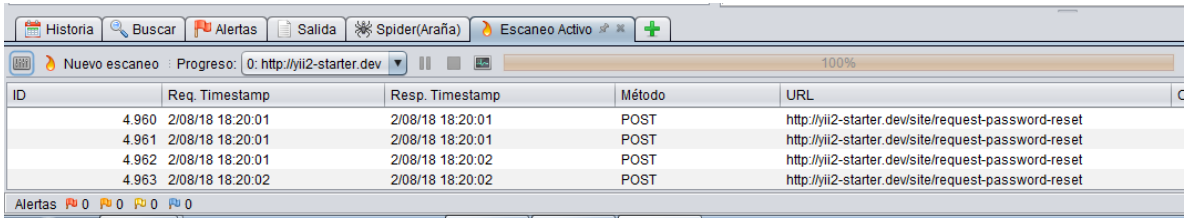


Ilustración 18 OWASP ZAP Resultado Final

Capítulo 6. Conclusiones y recomendaciones

Conclusiones

Se conoció a detalle el modelo de madurez en ciberseguridad ECM2, lo cual fue indispensable para desarrollar una aplicación web que lo reflejara de forma correcta.

Se identificaron los principales estándares utilizados en la industria del desarrollo de aplicaciones web, ello permitió el desarrollo de un producto confiable y seguro.

Se recopilaron las principales prácticas y técnicas para el desarrollo de aplicaciones web seguras descritas en los estándares identificados, esto permitió aplicar únicamente aquellas prácticas con un verdadero valor agregado a la aplicación desarrollada.

Se investigó la forma en que trabaja el proceso de autenticación de usuarios en aplicaciones web mediante el uso de firma digital, esto permitió su adecuada implementación en la aplicación web desarrollada, aportando un mayor nivel de seguridad y confiabilidad.

La elaboración de la arquitectura de la aplicación permitió identificar los diversos componentes; aplicación web, base de datos y servidores, así como sus características, necesarios para el adecuado funcionamiento de la misma.

Se determinó que existen herramientas de software libre; como MySql y Yii2 Framework, las cuales además del beneficio económico de no requerir la compra de licencias para su uso, ofrecen características de seguridad que las hacen robustas y atractivas.

Se logró el desarrollo de una aplicación web la cual permite a diversas organizaciones realizar autoevaluaciones en el campo de la ciberseguridad utilizando el modelo de madurez ECM2. Además, dicha aplicación cuenta con características que la hacen robusta y segura, por consiguiente brinda un grado de confiabilidad para los usuarios.

Las pruebas funcionales de la aplicación permitieron determinar si se implementó de forma correcta la automatización del modelo de ciberseguridad ECM2, además ayudaron en la evaluación de algunas de las características de seguridad incorporadas durante el desarrollo de la aplicación.

La utilización de herramientas automatizadas para la detección de vulnerabilidades en aplicaciones web, reducen el tiempo requerido para encontrar fallas en seguridad, además de minimizar error y sesgo humano.

Recomendaciones

1. Debido al panorama cambiante en ciberseguridad se recomienda a los administradores de la aplicación, mantener el modelo y la aplicación en constante revisión, con el objetivo de conservar su relevancia como herramienta valor estratégico en la toma de decisiones y asignación de recursos.
2. Se recomienda a los encargados de la aplicación velar por la constante actualización de las plataformas en donde se ejecuta la aplicación con el objetivo de minimizar el riesgo de vulnerabilidades y mantener la solución vigente.
3. Se recomienda a los usuarios el uso del certificado de firma digital, como método de autenticación por cuanto es más seguro que el de usuario y contraseña, con ello se minimiza la probabilidad de vulneración de las credenciales; además, les evita el estar recordando credenciales adicionales a las obtenidas.
4. Se recomienda a los usuarios, cuando existe más de una sede, aplicar el modelo a toda la institución de manera integral, con el objetivo de aprovechar la transmisión de conocimiento de una sede a otra y generar una política general de seguridad.
5. Es recomendable que la alta gerencia defina, con base en sus metas y objetivos, la periodicidad con la cual se deben aplicar las evaluaciones, con el objetivo de brindar seguimiento a los puntos de mejora identificados y detectar posibles debilidades lo más pronto posible. El darles trazabilidad a las evaluaciones no solo funciona como una fotografía de la seguridad, sino como un parámetro de referencia para la inversión y priorización de recursos.

Capítulo 7. Trabajos futuros

Debido al alcance global del modelo, que permite su utilización en cualquier institución independientemente del tamaño y sector, sería importante implementar internacionalización en la aplicación con el fin de potenciar su uso en otras latitudes, independiente de idioma.

Asimismo, en futuras versiones sería importante, agregar otros descriptores a las instituciones y sedes evaluadas, con el fin de realizar el análisis según el tipo (público, privado, sector, ubicación y tamaño).

Un punto a mejorar en futuras versiones sería la incorporación de un módulo de reportaría que otorgue mayor flexibilidad al usuario a la hora de extraer y generar informes.

Debido al dinamismo que caracteriza el sector de la ciberseguridad se recomienda, realizar constantes evaluaciones al modelo e ir realizando ajustes con el fin de mantener el modelo y la aplicación vigente y generar valor al usuario.

Bibliografía

Castellanos, T., Gallego, J. C., Delgado, J. A., & Merchán, L. (2014). *Análisis comparativo entre los modelos de madurez reconocidos en la gestión de proyectos.* Obtenido de Biblioteca Digital Universidad de San Buenaventura: http://bibliotecadigital.usb.edu.co/handle/10819/2163

Cevallos, K. (04 de 06 de 2015). *UML: Casos de Uso.* Obtenido de Ingeniería del Software: https://ingsotfwarekarlacevallos.wordpress.com/2015/06/04/uml-casos-de-uso/

Cevallos, K. (07 de 07 de 2015). *UML: Diagrama de Secuencia.* Obtenido de Ingeniería del Software: https://ingsotfwarekarlacevallos.wordpress.com/2015/07/07/uml-diagrama-de-secuencia/

Chacón Jiménez, K. (2016 de 09 de 2016). *Firma digital avanza con sigilo.* Obtenido de El Financiero: https://www.elfinancierocr.com/tecnologia/firma-digital-avanza-con-sigilo/3CUXU6RB7JEVHO6J2DXBQIFAHA/story/

Codina, L. (1998). Metodología de análisis de sistemas de información y de diseño de bases de datos documentales: aspectos lógicos y funcionales. *Anuario SOCADI de Documentación e Información: 1998*, 195-209.

Cordero, Z. R. (2009). LA INVESTIGACIÓN APLICADA: UNA FORMA DE CONOCER LAS REALIDADES CON EVIDENCIA CIENTÍFICA. *Revista Educación*, 159. Recuperado el 07 de 12 de 2017, de https://revistas.ucr.ac.cr/index.php/educacion/article/viewFile/538/589

Cortés Domínguez, J. (12 de 06 de 2017). *Ciberataques: La débil apuesta de las pymes por la seguridad informática.* Obtenido de Retina: https://retina.elpais.com/retina/2017/06/01/tendencias/1496307759_889133.html

Department of Homeland Security. (04 de 08 de 2014). *Cybersecurity Capability Maturity Model.* Obtenido de Official website of the Department of Homeland Security: https://niccs.us-cert.gov/sites/default/files/Capability%20Maturity%20Model%20White%20Paper.pdf?trackDocs=Capability%20Maturity%20Model%20White%20Paper.pdf

Dirección de Certificadores de Firma Digital Ministerio de Ciencia y Tecnología. (s.f.). *Firma Digital*. Recuperado el 26 de 11 de 2017, de http://www.firmadigital.go.cr: http://www.firmadigital.go.cr/firma.html

Eleanor A., V. T., Diana G., A. L., Iván L., A. G., & Jenniffer M., Y. L. (15 de 06 de 2017). *Hardening y diseño de un ambiente de virtualización para el manejo de múltiples servidores de VoIP sobre una misma plataforma.* Obtenido de Polo del conocimiento: https://polodelconocimiento.com/ojs/index.php/es/article/view/146

ISO. (10 de 2005). *ISO/IEC 15408-1:2005 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model.* Obtenido de International Organization for Standardization: https://www.iso.org/standard/40612.html

ISO 27000. (2012). *ISO 27000.es*. Obtenido de El portal de ISO 27001 en Español: http://www.iso27000.es/glosario.html

Kaspersky Lab. (13 de 08 de 2018). *Comunicados de prensa*. Obtenido de Kaspersky Lab: https://latam.kaspersky.com/about/press-releases/2018_panorama-de-

M., J. V. (04 de 2010). *Investigación bibliotecológica.* Recuperado el 24 de 11 de 2017, de Preservación documental digital y seguridad informática: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

Mendoza, M. Á. (16 de 06 de 2015). *¿Ciberseguridad o seguridad de la información? Aclarando la diferencia.* Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Menk III, C. G. (Junio de 1996). *System Security Engineering Capability Maturity Model and Evaluations: Partners Within the Assurance Framework.* Obtenido de The National Institute of Standards and Technology (NIST): https://csrc.nist.gov/csrc/media/publications/conference-paper/1996/10/22/proceedings-of-the-19th-nissc-1996/documents/paper010/cmmtpep.pdf

Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2017). Recuperado el 20 de 10 de 2017, de http://www.micit.go.cr/: http://www.micit.go.cr/index.php?option=com_content&view=featured&Itemid=669

Negro, R. P. (s.f.). *http://openaccess.uoc.edu.* Recuperado el 12 de 12 de 2017, de Universitat Oberta de Catalunya: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/14730/6/rpelaeznTFM0612memoria.pdf

NIST. (07 de 12 de 2016). *Program Review for Information Security Assistance*. Obtenido de NIST: https://csrc.nist.gov/projects/program-review-for-information-security-assistance/security-maturity-levels

OWASP. (s.f.). *Welcome to OWASP.*Obtenido de OWASP: https://www.owasp.org/index.php/Main_Page

OWASP., F. (2017). *Estándar de Verificación de Seguridad en aplicaciones Aplicaciones 3.0.1.* Obtenido de www.owasp.org: https://www.owasp.org/images/a/aa/Est%C3%A1ndar_de_Verificaci%C3%B3n_de_Seguridad_en_Aplicaciones_3.0.1.pdf

Porto, J. P., & Gardey, A. (2013). *Definición de manual de usuario.* Recuperado el 16 de 07 de 2018, de https://definicion.de/: https://definicion.de/manual-de-usuario/

Programa Sociedad de la Información y el Conocimiento PROSIC. (2012). *Hacia la sociedad de la información y el conocimiento : informe 2012.* Recuperado el 01 de 11 de 2017, de http://www.prosic.ucr.ac.cr/sites/default/files/recursos/informe_2012.pdf

Real Academia Española. (2017). *Real Academia Española.* Recuperado el 10 de 12 de 2017, de http://dle.rae.es: http://dle.rae.es/?id=4TO3M08

Rodríguez Bravo, C. A. (2017). *Creación de Modelo de Madurez en Ciberseguridad.* Tesis de Maestría, Cenfotec.

Symantec. (06 de 2014). *Tendencias de Seguridad Cibernética en América Latina y el Caribe.* Obtenido de Symantec: https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

U.S. Department of Energy (DOE). (2 de 2014). *Cybersecurity Capability Maturity Model (C2M2).*Recuperado el 12 de 12 de 2017, de Electricity Delivery & Energy Reliability: https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

Unión Internacional de Telecomunicaciones. (04 de 2008). *X.1205 : Aspectos generales de la ciberseguridad.* Obtenido de ITU: https://www.itu.int/rec/T-REC-X.1205-200804-I/es

Velasco, R. (25 de 04 de 2015). *OWASP ZAP, herramienta para auditar la seguridad de una página web*. Obtenido de RedesZone: https://www.redeszone.net/2015/04/25/seguridad-web-owasp-zap/

Voutssás M., J. (04 de 2010). *Preservación documental digital y seguridad informática.* Recuperado el 20 de 11 de 2017, de Investigación bibliotecológica: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

www.yiiframework.com. (20 de 07 de 2018). *Guía Definitiva de Yii 2.0*. Obtenido de www.yiiframework.com: https://www.yiiframework.com/doc/guide/2.0/es/intro-yii

Anexos

Anexo 1: Caso de uso

Creación de una plataforma web segura para automatizar el modelo de madurez en ciberseguridad ECM2 con el fin de facilitar la tarea de determinar el estado real en materia de ciberseguridad a instituciones sin importar su tamaño o sector

Descripción breve

Documento con especificación de casos de uso de las diferentes funcionalidades que debe contemplar la herramienta web para la Automatización del modelo de Ciberseguridad ECM2

Luis Humberto Pérez González
Marlon Soto Elizondo

Agregar institución

Caso de uso: Agregar Institución	
Nombre	Agregar institución
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Agregar institución
Actores	Usuario administrador
Precondiciones	El usuario debe estar registrado y autenticado como administrador. La institución no debe de estar registrada previamente.
Flujo Normal	1) El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Instituciones” 2) La aplicación despliega una tabla con la información de las instituciones registradas en la aplicación. 3) El actor presiona el botón “Agregar Institución” 4) La aplicación le muestra un formulario con el siguiente espacio a) Nombre de la Institución: Espacio requerido 5) El actor presiona el botón “Guardar” 6) La aplicación valida la información ingresada 7) La aplicación lo redirige a la página de catálogo de instituciones

	8) El caso de uso termina.
Caso de uso: Agregar institución	
Flujo Alternativo	1. El usuario puede cancelar la operación en cualquier momento del proceso presionando el botón “Cancelar” del formulario. 2. En caso de no completar el campo del formulario la aplicación debe advertir mediante un mensaje el faltante de dicho campo
Pos-condiciones	1. La aplicación automáticamente crea una sede por defecto para cada institución.

Actualizar institución

Caso de uso: Actualizar Institución	
Nombre	Actualizar institución
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Actualizar institución
Actores	Usuario administrador
Precondiciones	El usuario debe estar registrado y autenticado como administrador. La institución debe de estar registrada previamente.
Flujo Normal	1) El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Instituciones” 2) La aplicación despliega una tabla con la información de las instituciones registradas en la aplicación. 3) El actor presiona el botón “Actualizar” 4) La aplicación despliega un formulario con la información de la institución previamente ingresada 5) El usuario edita la información. 6) El actor presiona el botón “Guardar” 7) La aplicación valida la información ingresada

	8) La aplicación lo redirige a la página de catálogo de instituciones 9) El caso de uso termina.
Caso de uso: Actualizar institución	
Flujo Alternativo	1. El usuario puede cancelar la operación en cualquier momento del proceso presionando el botón “Cancelar” ubicado en el formulario. 2. En caso de no completar el campo del formulario la aplicación debe advertir mediante un mensaje el faltante de dicho campo

Eliminar institución

Caso de uso: Eliminar Institución	
Nombre	Eliminar institución
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Eliminar una institución
Actores	Usuario administrador
Precondiciones	El usuario debe estar registrado y autenticado como administrador. La institución debe de estar registrada previamente.

Flujo Normal	1) El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Instituciones” 2) La aplicación despliega una tabla con la información de las instituciones registradas en la aplicación. 3) El actor presiona el botón “Eliminar” 4) La aplicación emite una advertencia de corroboración si realmente desea llevar a cabo dicha operación. 5) El registro es eliminado 6) El caso de uso termina.
Caso de uso: Eliminar institución	
Flujo Alternativo	1. El usuario puede evitar la acción en el momento del mensaje corroboración de la acción de eliminado 2. La aplicación evita el eliminado en caso que tenga datos relacionados

Registrar usuarios

Caso de uso: Registrar usuarios	
Nombre	Registrar usuarios
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Registro de usuarios
Actores	Usuario administrador
Precondiciones	El usuario debe estar registrado y autenticado como administrador Debe existir en el sistema al menos una institución a la cual se pueda asociar el usuario.
Flujo Normal	1. El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Usuarios” 2. El actor presiona el botón de “Agregar usuario” 3. La aplicación muestra el formulario de registro de usuarios. 4. La aplicación solicita la siguiente información al actor: a) Identificación: Se debe ingresar el número de cedula del usuario (Sin espacios ni guiones) b) Nombre de usuario: Campo requerido c) Primer apellido: Campo requerido

	d) Segundo apellido e) Correo electrónico: Campo requerido f) Puesto g) Institución: Campo requerido 5. El actor debe proporcionar la información de registro, y presiona el botón “Guardar” que le permite finalizar el registro. 6. El sistema valida la información digitada. 7. El sistema registra el usuario, y lo dirige al catálogo de usuarios registrados 8. El caso de uso termina
Caso de uso: Registrar usuarios	
Flujo Alternativo	1. En caso que el actor, no desee continuar con el proceso de registro, este puede cancelar el proceso de registro presionando el botón “Cancelar” del formulario. 2. En caso que los datos proporcionados no se encuentren en el formato requerido el sistema debe notificar el formato deseado. 3. En caso que el usuario no complete los espacios requeridos el sistema debe mostrar mediante un mensaje los espacios

	faltantes.
Pos-condiciones	De cumplirse el paso 8, el usuario está listo para activarse.

Actualizar usuarios

Caso de uso: Actualizar usuario	
Nombre	Actualizar usuario
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Actualizar usuario
Actores	Usuario administrador
Precondiciones	El usuario debe estar registrado y autenticado como administrador
Flujo Normal	1) El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Usuarios” 2) La aplicación despliega una tabla con la información de los Usuarios registrados en la aplicación. 3) El actor presiona el botón “Actualizar” 4) El sistema muestra un formulario con la información agregada previamente. 5) El usuario puede modificar la información contenida en el formulario 6) El usuario presiona el botón “Guardar” en el formulario. 7) La aplicación valida que la información.

	8) La aplicación lo redirige al catálogo de usuarios 9) El caso de uso termina
Caso de uso: Actualizar usuario	
Flujo Alternativo	1. En caso que el actor, no desee continuar con el proceso de Actualización de usuario, este puede cancelar el proceso presionando el botón “Cancelar” presente en el formulario 2. En caso que el usuario no complete los espacios requeridos el sistema debe mostrar mediante un mensaje los espacios faltantes.

Eliminar usuarios

Caso de uso: Eliminar usuario	
Nombre	Eliminar usuario
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	La aplicación debe proveer de un módulo con la capacidad de eliminar usuarios
Actores	Usuario administrador

Precondiciones	El usuario debe estar registrado y autenticado como administrador. El usuario no debe poseer datos asociados.
Flujo Normal	1) El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Usuarios” 2) La aplicación despliega una tabla con la información de los usuarios registrados en la aplicación. 3) El actor debe presionar el icono Eliminar, ubicado en la columna acciones. 4) La aplicación pregunta si realmente desea llevar a cabo la acción. 5) Elimina el usuario. 6) El caso de uso termina
Caso de uso: Eliminar usuario	
Flujo Alternativo	1. En caso que el usuario que se desea eliminar posea datos asociados, la aplicación no permitir su eliminación. 2. La aplicación muestra con un mensaje con el motivo por el cual se evitó la eliminación del usuario

Cambiar estado de usuario

Caso de uso: Cambiar estado de usuario	
Nombre	Cambiar estado de usuario
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	La aplicación debe permitir a un usuario autenticado como administrador tener la posibilidad de activar o desactivar un usuario de la aplicación.
Actores	Usuario administrador
Precondiciones	El usuario debe estar registrado y autenticado como administrador
Flujo Normal	1. El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Usuarios” 2. La aplicación despliega una tabla con la información de los usuarios registrados en la aplicación. 3. El actor debe presionar el icono cambiar estado, ubicado en la columna “Acciones”. 4. La aplicación lo redirige a una pantalla en donde se muestra el detalle de la información del usuario seleccionado. 5. El actor presiona el botón “Cambiar estado” el cual activa o

	desactiva el usuario seleccionado. 6. Para la operación de activar usuario, la aplicación debe enviar un correo electrónico con un enlace para validar la cuenta y establecer una contraseña propia. 7. El caso de uso termina.
Caso de uso: Cambiar estado de usuario	
Flujo Alternativo	1. En caso que el actor no desee continuar con el proceso de activación de usuario el sistema debe proveer la opción de anular la operación presionando el botón “Cancelar” 2. En caso que la cuenta de usuario ya estuviera activa, la aplicación debe mostrar la opción de desactivar la cuenta.
Pos-condiciones	Una vez completado el paso 7 el usuario puede iniciar a hacer uso de la aplicación.

Agregar dominio

Caso de uso: Agregar dominio	
Nombre	Agregar dominio

Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Agregar un dominio
Actores	Usuario administrador
Precondiciones	El usuario debe estar registrado y autenticado como administrador
Flujo Normal	1) El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Dominios” 2) La aplicación despliega una tabla con la información de los Dominios registrados en la aplicación. 3) El actor presiona el botón “Agregar dominio” 4) La aplicación le muestra un formulario con los siguientes espacios a) Código: Espacio requerido. b) Nombre: Espacio requerido. 5) El actor presiona el botón “Guardar”. 6) La aplicación valida que la información ingresada. 7) La aplicación lo redirige al catálogo de dominios 8) El caso de uso termina
Caso de uso: Agregar dominio	
Flujo	1. En caso que el actor, no desee continuar con el proceso de

Alternativo	ingreso de dominio, este puede cancelar el proceso presionando el botón “Cancelar” presente en el formulario 2. En caso que el usuario no complete los espacios requeridos el sistema debe mostrar mediante un mensaje los espacios faltantes.

Actualizar dominio

Caso de uso: Actualizar dominio	
Nombre	Actualizar dominio
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Actualizar un dominio
Actores	Usuario administrador
Precondiciones	El usuario debe estar registrado y autenticado como administrador
Flujo Normal	1) El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Dominios” 2) La aplicación despliega una tabla con la información de los Dominios registrados en la aplicación. 3) El actor presiona el botón “Actualizar”.

	4) La aplicación muestra un formulario con los datos ingresados del dominio. 5) El usuario edita los campos que desea. 6) El usuario oprime el botón “Guardar” ubicado en el formulario. 7) El sistema valida los datos en el formulario 8) La aplicación lo redirige al catálogo de dominios 9) El caso de uso termina
Caso de uso: Actualizar dominio	
Flujo Alternativo	1. En caso que el actor, no desee continuar con el proceso de actualización de dominio, este puede cancelar el proceso presionando el botón “Cancelar” presente en el formulario 2. En caso que el usuario elimine la información contenida en los espacios requeridos el sistema debe mostrar mediante un mensaje los espacios faltantes

Eliminar dominio

Caso de uso: Eliminar dominio	
Nombre	Eliminar dominio

Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Eliminar un dominio
Actores	Usuario administrador
Precondiciones	El usuario debe estar registrado y autenticado como administrador El dominio no debe poseer ninguna información asociada (Controles, Niveles)
Flujo Normal	1) El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Dominios” 2) La aplicación despliega una tabla con la información de los Dominios registrados en la aplicación. 3) El actor presiona el botón “Eliminar”. 4) La aplicación corrobora si el usuario desea efectuar la acción. 5) Se elimina el dominio. 6) El caso de uso termina.
Caso de uso: Eliminar dominio	
Flujo Alternativo	1. En caso que el dominio se encuentre siendo utilizado por algún control, la aplicación impide su eliminación. 2. El sistema alerta al usuario el motivo por el cual la acción no se

puede efectuar.

Agregar control

Caso de uso: Agregar control	
Nombre	Agregar control
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Agregar un control
Actores	Usuario interno
Precondiciones	El usuario debe estar registrado y autenticado como administrador
Flujo Normal	1) El caso de uso inicia cuando el usuario inicia sesión en el módulo de administrador. 2) El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Controles” 3) La aplicación despliega una tabla con la información de los Controles registrados en la aplicación. 4) El actor presiona el botón “Agregar control” 5) La aplicación le muestra un formulario con los siguientes espacios

	a) Código: Espacio requerido. b) Nombre: Espacio requerido. c) Opción para seleccionar el dominio al que pertenece: Espacio requerido 6) El actor presiona el botón “Guardar”. 7) La aplicación valida que la información ingresada. 8) La aplicación lo redirige al catálogo de controles 9) El caso de uso termina
Caso de uso: Agregar control	
Flujo Alternativo	1. En caso que el actor, no desee continuar con el proceso para ingresar un control, este puede cancelar el proceso presionando el botón “Cancelar” presente en el formulario 2. En caso que el usuario no complete los espacios requeridos el sistema debe mostrar mediante un mensaje los espacios faltantes.

Actualizar control

Caso de uso: Actualizar control

Nombre	Actualizar control
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Actualizar control
Actores	Usuario administrador
Precondiciones	El usuario debe estar registrado y autenticado como administrador
Flujo Normal	1) El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Controles” o bien desde el acceso directo en el panel de administración. 2) La aplicación despliega una tabla con la información de los Controles registrados en la aplicación. 3) El actor presiona el botón “Actualizar”. 4) La aplicación muestra un formulario con los datos ingresados para el control. 5) El usuario edita los campos que desea. 6) El usuario oprime el botón “Guardar” ubicado en el formulario. 7) El sistema valida los datos en el formulario 8) La aplicación lo redirige al catálogo de controles 9) El caso de uso termina

Caso de uso: Actualizar control	
Flujo Alternativo	1. En caso que el actor, no desee continuar con el proceso de actualización el control, este puede cancelar el proceso presionando el botón “Cancelar” presente en el formulario 2. En caso que el usuario elimine la información contenida en los espacios requeridos el sistema debe mostrar mediante un mensaje los espacios faltantes

Eliminar control

Caso de uso: Eliminar control	
Nombre	Eliminar control
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Eliminar un control
Actores	Usuario administrador
Precondiciones	El usuario debe estar registrado y autenticado como administrador El control no debe poseer ninguna información asociada (Niveles, evaluaciones)
Flujo Normal	1) El actor ingresa al menú “Mantenimientos” y selecciona la opción

	de “Controles” 2) La aplicación despliega una tabla con la información de los Controles registrados en la aplicación. 3) El usuario selecciona un control 4) El actor presiona el botón “Eliminar”. 5) La aplicación corrobora si el usuario desea efectuar la acción. 6) Se elimina el control. 7) El caso de uso termina.
Caso de uso: Eliminar control	
Flujo Alternativo	3. En caso que el control se encuentre siendo utilizado por algún nivel o evaluación, la aplicación impide su eliminación. 4. El sistema alerta al usuario el motivo por el cual la acción no se puede efectuar.

Agregar niveles

Caso de uso: Agregar niveles	
Nombre	Agregar niveles

Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Agregar niveles
Actores	Usuario administrador
Precondiciones	El usuario debe estar registrado y autenticado como administrador. Debe existir al menos un control previamente ingresado
Flujo Normal	1) El caso de uso inicia cuando el usuario inicia sesión en el módulo de administrador. 2) El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Niveles” 3) La aplicación despliega una tabla con la información de los niveles registrados en la aplicación. 4) El actor presiona el botón “Agregar niveles” 5) La aplicación le muestra un formulario con el siguiente espacio a) Valor: Espacio requerido b) Descripción: Espacio requerido c) Opción de seleccionar el control al que pertenece el nivel: Espacio requerido 6) El actor presiona el botón “Guardar” 7) La aplicación valida la información ingresada

	8) La aplicación lo redirige a la página de catálogo de los niveles 9) El caso de uso termina.
Caso de uso: Agregar niveles	
Flujo Alternativo	3. El usuario puede cancelar la operación en cualquier momento del proceso presionando el botón “Cancelar” ubicado en el formulario. 4. En caso de no completar el campo del formulario la aplicación debe advertir mediante un mensaje el faltante de dicho campo
Pos-condiciones	2. La aplicación automáticamente crea una sede por defecto para cada institución. 3. La aplicación esta lista para poder asociar un usuario a la institución.

Actualizar nivel

Caso de uso: Actualizar nivel	
Nombre	Actualizar nivel
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018

Descripción	Actualizar nivel
Actores	Usuario interno
Precondiciones	El usuario debe estar registrado y autenticado como administrador
Flujo Normal	1) El caso de uso inicia cuando el usuario inicia sesión en el módulo de administrador. 2) El actor ingresa al menú “Mantenimientos” y selecciona la opción de “Niveles” o bien desde el acceso directo en el panel de administración. 3) La aplicación despliega una tabla con la información de los Niveles registrados en la aplicación. 4) El actor presiona el botón “Actualizar”. 5) La aplicación muestra un formulario con los datos ingresados para el nivel. 6) El usuario edita los campos que desea. 7) El usuario oprime el botón “Guardar” ubicado en el formulario. 8) El sistema valida los datos en el formulario 9) La aplicación lo redirige al catálogo de niveles 10) El caso de uso termina

Caso de uso: Actualizar nivel

Flujo Alternativo	1. En caso que el actor, no desee continuar con el proceso de actualización de nivel, este puede cancelar el proceso presionando el botón “Cancelar” presente en el formulario 2. En caso que el usuario elimine la información contenida en los espacios requeridos el sistema debe mostrar mediante un mensaje los espacios faltantes

Eliminar nivel

Caso de uso: Eliminar nivel	
Nombre	Eliminar nivel
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Eliminar un nivel
Actores	Usuario interno
Precondiciones	El usuario debe estar registrado y autenticado como administrador El nivel no debe poseer ninguna información asociada (evaluaciones)
Flujo Normal	1) El actor ingresa al menú “Mantenimientos” y selecciona la opción de “niveles” 2) La aplicación despliega una tabla con la información de los niveles

	registrados en la aplicación. 3) El usuario selecciona un nivel 4) El actor presiona el botón “Eliminar”. 5) La aplicación corrobora si el usuario desea efectuar la acción. 6) Se elimina el nivel. 7) El caso de uso termina.
Caso de uso: Eliminar control	
Flujo Alternativo	1. En caso que el nivel se encuentre siendo utilizado por alguna evaluación, la aplicación impide su eliminación. 2. El sistema alerta al usuario el motivo por el cual la acción no se puede efectuar.

Agregar sede

Caso de uso: Agregar sede	
Nombre	Agregar sede
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018

Descripción	Agrega una sede a una institución.
Actores	Usuario externo
Precondiciones	El usuario debe estar registrado y autenticado en la aplicación.
Flujo Normal	1) El usuario presiona el ítem de menú “Sedes”, ubicado en el menú principal 2) La aplicación muestra el catálogo de las Sedes que posee la institución. 3) El actor presiona el botón “Agregar sede” 4) La aplicación muestra un formulario donde se debe agregar la información. 5) El usuario agrega la información al formulario 6) El actor presiona el botón “Guardar” 7) La aplicación valida los datos ingresados 8) La aplicación re direcciona al catálogo de sedes 9) El caso de uso termina.
Caso de uso: Agregar sede	
Flujo Alternativo	1. El usuario puede evitar la acción en el momento presionando el botón “Cancelar” localizado en el formulario.

Actualizar sede

Caso de uso: Actualizar sede	
Nombre	Actualizar sede
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Actualizar una sede previamente registrada
Actores	Usuario externo
Precondiciones	El usuario debe estar registrado y autenticado en la aplicación.
Flujo Normal	1) El usuario presiona el ítem de menú “Sedes”, ubicado en el menú principal 2) La aplicación muestra el catálogo de las Sedes que posee la institución. 3) El actor presiona el botón “Actualizar” 4) La aplicación muestra los datos previamente ingresados. 5) El usuario modifica los valores del formulario. 6) El actor presiona el botón “Guardar” 7) La aplicación valida la información del formulario. 8) La aplicación redirecciona al catálogo de sedes 9) El caso de uso termina.

Caso de uso: Actualizar sede	
Flujo Alternativo	2. El usuario puede evitar la acción en el momento presionando el botón “Cancelar” localizado en el formulario.

Eliminar sede

Caso de uso: Eliminar sede	
Nombre	Eliminar sede
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Eliminar una sede previamente registrada
Actores	Usuario externo
Precondiciones	El usuario debe estar registrado y autenticado en la aplicación.
Flujo Normal	1) El usuario presiona el ítem de menú “Sedes”, ubicado en el menú principal 2) La aplicación muestra el catálogo de las Sedes que posee la institución. 3) Selecciona la sede que desea eliminar. 4) El actor presiona el botón “Eliminar”

	5) La aplicación emite un mensaje que corrobore que el usuario realmente desea llevar a cabo la acción. 6) El registro es eliminado. 7) El caso de uso termina.
Caso de uso: Eliminar sede	
Flujo Alternativo	3. El usuario puede evitar la acción en el momento presionando el botón “Cancelar” en la advertencia de corroboración. 4. En caso que la sede posea datos asociados el sistema evita su eliminación y le muestra un mensaje con las razones al usuario.

Autenticación usuario contraseña

Caso de uso: Autenticación usuario contraseña	
Nombre	Autenticación usuario y contraseña
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Inicio de sesión en la aplicación mediante usuario y contraseña
Actores	Usuario externo/ Usuario administrador

Precondiciones	El usuario debe estar registrado en la aplicación
Flujo Normal	1) El usuario presiona el enlace e iniciar sesión 2) El usuario selecciona el mecanismo de inicio de sesión (Usuario contraseña/ firma digital) 3) El sistema le muestra un formulario con los siguientes espacios a) Usuario b) Contraseña 4) El usuario presiona el botón “Iniciar sesión” 5) El actor ingresa a la aplicación. 6) El caso de uso termina.

Caso de uso: Autenticación usuario y contraseña	
Flujo Alternativo	1. En caso de que los espacios del formulario no cumplan con el formato requerido el sistema deberá notificar la falta. 2. El usuario tiene la posibilidad de elegir el proceso de autenticación por medio de la firma digital

Autenticación firma digital

Caso de uso: Autenticación firma digital	
Nombre	Autenticación firma digital

Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Inicio de sesión en la aplicación mediante el uso de la firma
Actores	Usuario externo/ Usuario administrador
Precondiciones	El usuario debe estar registrado en la aplicación y tener habilitada la opción de ingresar por medio de firma
Flujo Normal	1) El usuario presiona el enlace e iniciar sesión 2) El usuario selecciona el mecanismo de inicio de sesión (Usuario contraseña/ firma digital) 3) El usuario selecciona la opción de iniciar sesión mediante firma digital 4) El usuario agrega la tarjeta de firma digital al dispositivo lector 5) El sistema muestra una ventana emergente donde debe agregar la contraseña de la firma digital 6) El usuario presiona el botón “Validar” 7) El actor ingresa a la aplicación. 8) El caso de uso termina.
Caso de uso: Autenticación usuario y contraseña	
Flujo	1. En caso que no se cuente con un certificado de firma

Alternativo	electrónica valido o que el “pin” del certificado no fuera el correcto la aplicación debe mostrar un mensaje con la descripción de lo sucedido

Recuperar contraseña

Caso de uso: Recuperar contraseña	
Nombre	Recuperar contraseña
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Recuperar contraseña en caso de olvido
Actores	Usuario externo/ Usuario administrador
Precondiciones	El usuario debe estar registrado en la aplicación y tener la opción de inicio de sesión por medio de usuario y contraseña
Flujo Normal	1) El usuario presiona el enlace de “Iniciar sesión” 2) El usuario selecciona el mecanismo de inicio de sesión (Usuario contraseña)

	3) El usuario da clic sobre el enlace de “Restablecer contraseña” 4) El sistema le muestra un nuevo formulario, donde debe ingresar el correo electrónico con el cual se registró en la aplicación 5) La aplicación le envía un correo electrónico con un enlace e instrucciones para restablecer la contraseña 6) El usuario recibe el correo electrónico con el enlace, oprime el vínculo y lo dirige a un formulario donde puede digitar una nueva contraseña 7) La aplicación valida el formato de la contraseña. 8) El sistema le muestra un mensaje si la operación se completa con éxito. 9) El caso de uso termina.
Caso de uso: Recuperar contraseña	
Flujo Alternativo	1. En caso de no recordar el correo electrónico con el cual se encuentra registrado en el sistema el usuario debe comunicarse con el administrador del sistema mediante el formulario de contacto o por algún otro medio, con el fin de recibir soporte

Agregar evaluación

Caso de uso: Agregar evaluación	
Nombre	Agregar una evaluación
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Realizar una evaluación aplicando el modelo de ciberseguridadECM2 sobre una sede en particular
Actores	Usuario externo
Precondiciones	El usuario debe estar registrado y autenticado en la aplicación
Flujo Normal	1) El usuario presiona el ítem de menú “Evaluaciones” 2) El sistema lo re direcciona a una nueva pantalla donde se ubican las evaluaciones anteriores en caso de contar con estas. 3) El usuario presiona el botón “Crear evaluación” 4) El usuario selecciona la sede donde desea aplicar la evaluación y completa una breve descripción u observación sobre la evaluación 5) El sistema lo re direcciona a una pantalla en donde se encuentra los diferentes dominios a evaluar. 6) El usuario oprime el botón evaluar en el dominio que desea analizar. 7) La aplicación muestra una serie de preguntas con respuestas de selección única además capacidad de agregar una observación u

	comentario sobre cada una de estas. 8) Una vez que el usuario completa las preguntas para el dominio y presiona el botón “Guardar” la aplicación lo re direcciona a la página de inicio de la evaluación donde se encuentran los restantes dominios. 9) La aplicación provee en tiempo real una gráfica con el resumen de las respuestas brindadas 10) Las aplicaciones conformes se van completando los dominios va otorgando una nota tanto al dominio como a la evaluación en general 11) La evaluación termina cuando el usuario evalúa la totalidad de dominios. 12) El caso de uso termina.
Caso de uso: Agregar evaluación	
Flujo Alternativo	1. El usuario puede presionar el botón “Cancelar” que se encuentra ubicado en los diferentes formularios y anular el proceso de evaluación 2. En caso de no completar la descripción u observación u omitir la selección de la sede a evaluar el sistema debe alertar al

usuario sobre tal condición.

Actualizar evaluación

Caso de uso: Actualizar evaluación	
Nombre	Actualizar una evaluación
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Actualizar una evaluación
Actores	Usuario externo
Precondiciones	El usuario debe estar registrado y autenticado en la aplicación
Flujo Normal	1) El usuario presiona el ítem de menú “Evaluaciones” 2) El sistema lo re direcciona a una nueva pantalla donde se ubican las evaluaciones realizadas. 3) El usuario elige la evaluación que desea actualizar 4) Presiona el botón “Ver detalles” 5) La aplicación lo redirige a la pantalla de inicio de la evaluación, en donde se visualizan todos los dominios. 6) El usuario selecciona el o los dominios que desea actualizar. 7) Para ingresar al dominio presiona el botón “Ver detalles”

	8) Cambia el valor de las respuestas que desea. 9) El usuario presiona el botón “Guardar”. 10) El caso de uso termina.
Caso de uso: Actualizar evaluación	
Flujo Alternativo	1. El usuario puede presionar el botón “Cancelar” que se encuentra en el formulario y anular la operación en cualquier momento.

Consultar evaluación

Caso de uso: Consultar evaluación	
Nombre	Consultar una evaluación
Autor	Marlon Soto Elizondo - Humberto Pérez González
Fecha	13-07-2018
Descripción	Consultar una evaluación
Actores	Usuario externo
Precondiciones	El usuario debe estar registrado y autenticado en la aplicación
Flujo Normal	1) El usuario presiona el ítem de menú “Evaluaciones” 2) El sistema lo re direcciona a una nueva pantalla donde se ubican

las evaluaciones realizadas.

3) El usuario elige la evaluación que desea consultar
4) Presiona el botón “Ver detalles”
5) La aplicación lo redirige a la pantalla de inicio de la evaluación, en donde se visualizan todos los dominios en cada dominio el usuario puede encontrar la nota del dominio, además al final de la evaluación el usuario puede consultar la nota global de la evaluación. En cada dominio además de la nota el usuario puede ver una representación gráfica de las respuestas emitidas.
6) El caso de uso termina.

Anexo 2: Diccionario de datos

Creación de una plataforma web segura para automatizar el modelo de madurez en ciberseguridad ECM2 con el fin de facilitar la tarea de determinar el estado real en materia de ciberseguridad a instituciones sin importar su tamaño o sector

Descripción breve

Documento con el nombre de las tablas, estructura y especificación de campos y tipos de datos de la base de datos para la automatización del modelo de ciberseguridad ECM2

Luis Humberto Pérez González

Marlon Soto Elizondo

Tabla: instituciones						
Observaciones	Catálogo de instituciones sobre las cuales se podrán realizar evaluaciones de ciberseguridad.					
Columnas						
Nombre	**Tipo Dato**	**Nulo**	**PK**	**FK**	**Default**	**Observaciones**
Id_Institucion	INT(11)	Si	Si	No		Identificador único de la institución. Autoincrementado
Nombre	VARCHAR(100)	Si	No	No		Nombre de la Institución.

Tabla: sedes						
Observaciones	Catálogo de sedes asociadas a las diferentes instituciones. Una institución puede tener una o más sedes sobres las que se realizan las evaluaciones de ciberseguridad.					
Columnas						
Nombre	**Tipo Dato**	**Nulo**	**PK**	**FK**	**Default**	**Observaciones**
Id_Sede	INT(11)	Sí	Sí	No		Identificador único

						de las sedes. Autoincrementado
Nombre	VARCHAR(100)	Sí	No	No		Nombre de la Sede
Ubicación	VARCHAR(250)	No	No	No	NULL	Ubicación geográfica.
Id_Institucion	INT(11)	Sí	No	Sí		Identificador único de la Institución a la que pertenece.
Fecha_Creacion	DATETIME	Sí	No	No	CURRENT_TIMESTAMP	Fecha de creación del registro.
Id_Usuario	INT(11)	Sí	No	Sí		Usuario que crea el registro.

Tabla: evaluaciones						
Observaciones	Catálogo de evaluaciones del modelo de ciberseguridad que se realizan las diferentes sedes de las instituciones.					
Columnas						
Nombre	**Tipo Dato**	**Nulo**	**PK**	**FK**	**Default**	**Observaciones**
Id_Evaluacion	INT(11)	Sí	Sí	No		Identificador único de la evaluación. Autoincrementado.
Consecutivo	INT(11)	No	No	No	NULL	Consecutivo de evaluación relacionado a la sede evaluada.
Fecha	DATETIME	No	No	No	CURRENT_TIMESTAMP	Fecha de creación del registro.
Status	TINYINT(1)	No	No	No	NULL	Estado de la evaluación: 0 Incompleta, 1 completada.

Id_Usuario	INT(11)	Sí	No	Sí		Usuario que crea el registro.
Id_Sede	INT(11)	Sí	No	Sí		Sede sobre la cual se realiza la evaluación.
Fecha_Ultima_Modificacion	DATETIME	No	No	No	CURRENT_TIMESTAMP	Fecha de última modificación del registro.
descripción	VARCHAR(250)	Sí	No	No		Descripción o nombre de la evaluación.

Tabla: dominios						
Observaciones	Catálogo de dominios de ciberseguridad que contempla el modelo ECM2					
Columnas						
Nombre	**Tipo Dato**	**Nulo**	**PK**	**FK**	**Default**	**Observaciones**

Id_Dominio	INT(11)	Sí	Sí	No		Identificador único del dominio. Autoincrementado
Nombre	VARCHAR(100)	Sí	No	No		Nombre o descripción del dominio.
Codigo	VARCHAR(5)	Sí	No	No		Código del dominio.

Tabla: controles						
Observaciones	Catálogo de controles de ciberseguridad asociados a los dominios del modelo ECM2.					
Columnas						
Nombre	**Tipo Dato**	**Nulo**	**PK**	**FK**	**Default**	**Observaciones**
Id_Control	INT(11)	Sí	Sí	No		Identificador único del control. Autoincrementado
Nombre	VARCHAR(100)	Sí	No	No		Nombre del control.
Id_Dominio	INT(11)	Sí	No	Sí		Identificador del dominio al que está asociado el control.
Código	VARCHAR(10)	Sí	No	No		Código del control.

Tabla: niveles	
Observacio nes	Niveles de madurez asociados a los diferentes controles del modelo de ciberseguridad ECM2.
Columnas	

Nombre	Tipo Dato	Nulo	PK	FK	Default	Observaciones
Id_Nivel	INT(11)	Sí	Sí	No		Identificador único del nivel. Autoincrementado.
Valor	INT(11)	No	No	No	NULL	Valor o calificación asignada al nivel, 0 la más baja, 4 la más alta, -1 queda reservado para No aplica (N/A)
Descripcion	VARCHAR(250)	No	No	No	NULL	Descripción del nivel.
Id_Control	INT(11)	Sí	No	Sí		Identificador único del control al que se asocia.

Tabla: respuestas						
Observaciones	Catálogo en el que se almacenan las respuestas de las evaluaciones asociadas a una institución-sede.					
Columnas						
Nombre	**Tipo Dato**	**Nulo**	**PK**	**FK**	**Default**	**Observaciones**
Id_Respuesta	INT(11)	Sí	Sí	No		Identificador único asociado a la respuesta. Autoincrementado.
Observaciones	VARCHAR(300)	No	No	No	NULL	Observaciones relacionadas a la respuesta.
Id_Nivel	INT(11)	Sí	No	Sí		Identificador del nivel seleccionado en la respuesta.
Id_Evaluacion	INT(11)	Sí	No	Sí		Identificador de le evaluación a la que se relaciona.
Id_Control	INT(11)	Si	No	Si		Identificador del control

						que se evalúa

Tabla: menu						
Observaciones	Catálogo de las diferentes rutas o Urls a las que tienen acceso los usuarios.					
Columnas						
Nombre	**Tipo Dato**	**Nulo**	**PK**	**FK**	**Default**	**Observaciones**
id	INT(11)	Sí	Sí	No		Identificador.
Nombre	VARCHAR(128)	Sí	No	No		Nombre de la ruta del menú.
parent	INT(11)	No	No	Sí	NULL	Identificador de menú padre.
route	VARCHAR(255)	No	No	No	NULL	Ruta o URL.
order	INT(11)	No	No	No	NULL	Orden aparición.
data	BLOB	No	No	No	NULL	

Tabla: user						
Observaciones	Catálogo de usuarios del sistema.					
Columnas						
Nombre	**Tipo Dato**	**Nulo**	**PK**	**FK**	**Default**	**Observaciones**
id	INT(11)	Sí	Sí	No		Identificador único del usuarios para el sistema. Autoincrementado.
username	VARCHAR(255)	Sí	No	No		Identificador único o Nombre de usuario. Para este caso el número de cédula del usuario.
Nombre	VARCHAR(50)	Sí	No	No		Nombre del usuario.
Apellido1	VARCHAR(30)	Sí	No	No		Primero apellido.
Apellido2	VARCHAR(30)	Sí	No	No		Segundo apellido.
Puesto	VARCHAR(100)	Sí	No	No		Puesto en la institución.
auth_key	VARCHAR(32)	Sí	No	No		Contraseña cifrada del usuario.

password_hash	VARCHAR(255)	Sí	No	No		Hash asociado a la contraseña del usuario.
password_reset_token	VARCHAR(255)	No	No	No	NULL	Token para reseteo de contraseña.
email	VARCHAR(255)	Sí	No	No		Correo electrónico del usuario.
status	SMALLINT(6)	Sí	No	No	'10'	Estado del usuario: 10 Activo, 0 Inactivo.
created_at	INT(11)	Sí	No	No		Fecha de creación del usuario.
updated_at	INT(11)	Sí	No	No		Fecha de actualización de los usuarios.
Id_Institucion	INT(11)	Sí	No	Sí		Identificador de la institución a la que pertenece el usuario.

Tabla: login_attempt						
Observaciones	Catálogo para el manejo de intentos de inicio de sesión, en caso de que un usuario falle 4 veces será bloqueado por un período de tiempo.					
Columnas						
Nombre	**Tipo Dato**	**Nulo**	**PK**	**FK**	**Default**	**Observaciones**
id	INT(11)	Sí	Sí	No		Identificador único del registro. Autoincrementado.
key	VARCHAR(255)	Sí	No	No		Contraseña en modo cifrado que digitó el usuario.
amount	INT(2)	No	No	No	'1'	Número de intento fallido.
reset_at	INT(11)	No	No	No	NULL	Fecha y hora en que se habilitará un usuario bloqueado.
updated_at	INT(11)	No	No	No	NULL	Fecha y hora del último intento fallido por iniciar sesión.

created_at	INT(11)	No	No	No	NULL	Fecha de creación del registro, o sea, fecha en que el usuario falló al iniciar sesión.

Tabla: auth_item						
Observaciones	Catálogo en el que se definen las funciones que podrán realizar los usuario, ejemplo operaciones, roles y tareas.					
Columnas						
Nombre	**Tipo Dato**	**Nulo**	**PK**	**FK**	**Default**	**Observaciones**
name	VARCHAR(64)	Si	Si	No		Nombre del ítem.
type	SMALLINT(6)	Si	No	No		0 = operación, 1 = tarea, 2 = rol.
description	TEXT	No	No	No	NULL	Descripción
rule_Nombre	VARCHAR(64)	No	No	Si	NULL	Nombre de la regla

						asociada.
data	BLOB	No	No	No	NULL	Regla de negocios asociada.
created_at	INT(11)	No	No	No	NULL	Fecha creación.
updated_at	INT(11)	No	No	No	NULL	Fecha de última actualización.

Tabla: auth_assignment

Observaciones	Catálogo para asignar permisos al usuario. Se pueden asignar diferentes roles a un usuario y cada uno de estos roles se almacena en el campo del nombre del elemento junto con otros valores como tareas, operaciones.

Columnas

Nombre	Tipo Dato	Nulo	PK	FK	Default	Observaciones
item_name	VARCHAR(64)	Sí	Sí	Sí		Identificador del Item: Rol, tarea, operación.
user_id	VARCHAR(64)	Sí	Sí	No		Identificación del usuario.

created_at	INT(11)	No	No	No	NULL	Fecha de creación del registro.

Tabla: auth_item_child

Observaciones	Catálogo para asignar operaciones tipo jerárquicos.					
Columnas						
Nombre	**Tipo Dato**	**Nulo**	**PK**	**FK**	**Default**	**Observaciones**
parent	VARCHAR(64)	Sí	Sí	Sí		Identificador del Item padre, por ejemplo un rol.
child	VARCHAR(64)	Sí	Sí	Sí		Identificador del Item hijo, por ejemplo una tarea del rol.

Tabla: auth_rule

Observaciones	Catálogo para reglas de autenticación.					
Columnas						
Nombre	**Tipo Dato**	**Nulo**	**PK**	**FK**	**Default**	**Observaciones**
Nombre	VARCHAR(64)	Sí	Sí	No		Nombre de la regla.
data	BLOB	No	No	No	NULL	
created_at	INT(11)	No	No	No	NULL	Fecha de creación
updated_at	INT(11)	No	No	No	NULL	Fecha de última actualización.

Tabla: migration

Observaciones	Tabla del frameworkYii en la cual se almacena información de las diferentes actualizaciones de los paquetes y complementos asociados al proyecto.

Columnas

Nombre	Tipo Dato	Nulo	PK	FK	Default	Observaciones
version	VARCHAR(180)	Sí	Sí	No		Número de versión del paquete.
apply_time	INT(11)	No	No	No	NULL	Fecha en que se aplicó la actualización.

nexo 3: Manual de usuario

Anexo 3: Manual de usuario

Creación de una plataforma web segura para automatizar el modelo de madurez en Ciberseguridad ECM2, con el fin de facilitar la tarea de determinar el estado real en esta materia a instituciones sin importar su tamaño o sector

Descripción breve

Documento con las instrucciones para el uso adecuado de cada uno de los módulos de la aplicación web tanto por parte del administrador, como de los usuarios externos pertenecientes a cada una de las instituciones registradas.

Luis Humberto Pérez González
Marlon Soto Elizondo

Introducción

El presente manual tiene como objetivo mostrar las pautas para la correcta operación de la aplicación ECM2. Después de leer este documento, el usuario podrá ser capaz alimentar con contenido los diferentes mantenimientos, realizar consultas, y confeccionar evaluaciones, a las diferentes instituciones y sedes, aplicando el modelo de madurez en Ciberseguridad ECM2

Acerca de la aplicación

ECM2es una aplicación que permite la automatización del modelo de madurez en Ciberseguridad ECM2, desarrollado por el Ingeniero Msc. César Rodríguez Bravo. Dicha aplicación tiene como objetivo facilitar la tarea de determinar el estado real, en que se encuentran las instituciones en materia de ciberseguridad, independientemente del tamaño o sector.

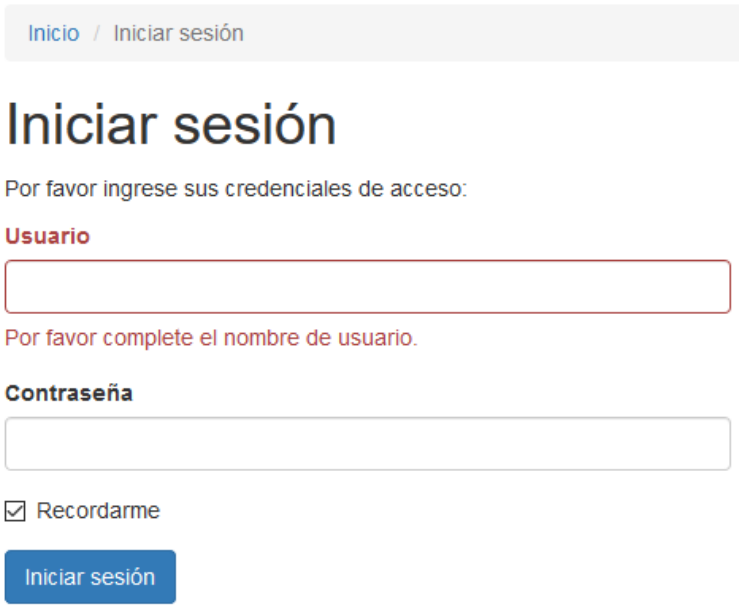
En cuanto a las estructura del aplicativo, está compuesta por dos secciones, un apartado para administradores, en la cual podrán realizar consultas y modificaciones a cada una de las secciones que conforman el modelo de ciberseguridad, y otra sección enfocada en el usuario externo en la cual este podrá aplicar el modelo en su institución o sede, e ir recibiendo retroalimentación en tiempo real.

Acceso al panel de administración

Para el ingreso al panel de administración es necesario que el usuario se autentique en la aplicación, para realizar esto el usuario cuenta con dos posibilidades, ingreso mediante usuario y contraseña o por medio del uso de firma digital. Para cualquiera de las dos modalidades es necesario que el administrador de la plataforma envié una invitación inicial mediante un correo electrónico.

Ingreso mediante usuario y contraseña

Para acceder al panel de administración, el usuario debe ingresar a la dirección electrónica de la aplicación web, y digitar su usuario y contraseña.



El formato del espacio usuario debe ser numeral y este debe de coincidir con el número de cédula o DIMEX (Documento de identidad migratoria para extranjeros) en caso de los extranjeros. Solo son permitidos caracteres numéricos, no se deben incluir espacios o guiones. Ejemplo del formato 205790823.

Para el caso de la contraseña esta debe tener un mínimo de seis caracteres. Se recomienda que estas no sean ni números ni letras consecutivas, o estar relacionadas con información personal como números de teléfonos, fechas de nacimiento, nombre de mascota o familiares cercanos.

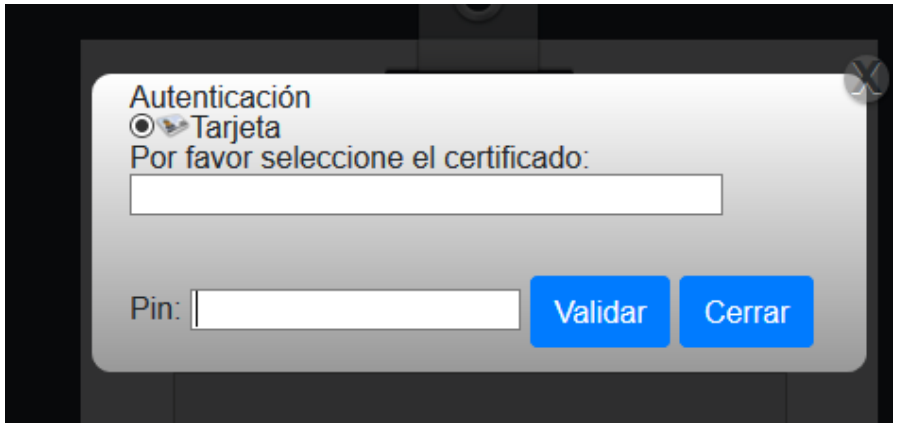
Es importante recordar que las credenciales son de uso personal y deben ser mantenidas en secreto, no se recomienda anotarlas o compartidas con algún un tercero.

Ingreso mediante firma digital

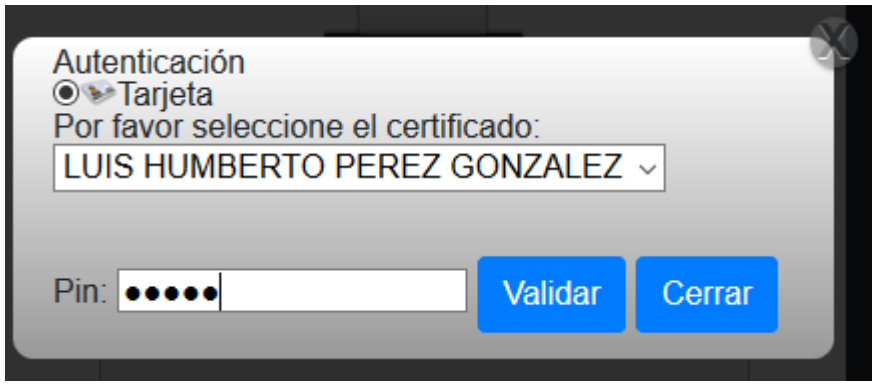
Para ingresar al panel de administración, el usuario tiene la opción de hacerlo mediante el uso del certificado de firma digital. Para hacerlo por medio de esta alternativa el administrador de la plataforma debe haber autorizado previamente esta opción.

El usuario debe ingresar a la dirección electrónica de la aplicación web y presionar la opción de firma digital.

Una vez presionado el botón de firma digital aparecerá una ventana emergente solicitando el ingreso del certificado.

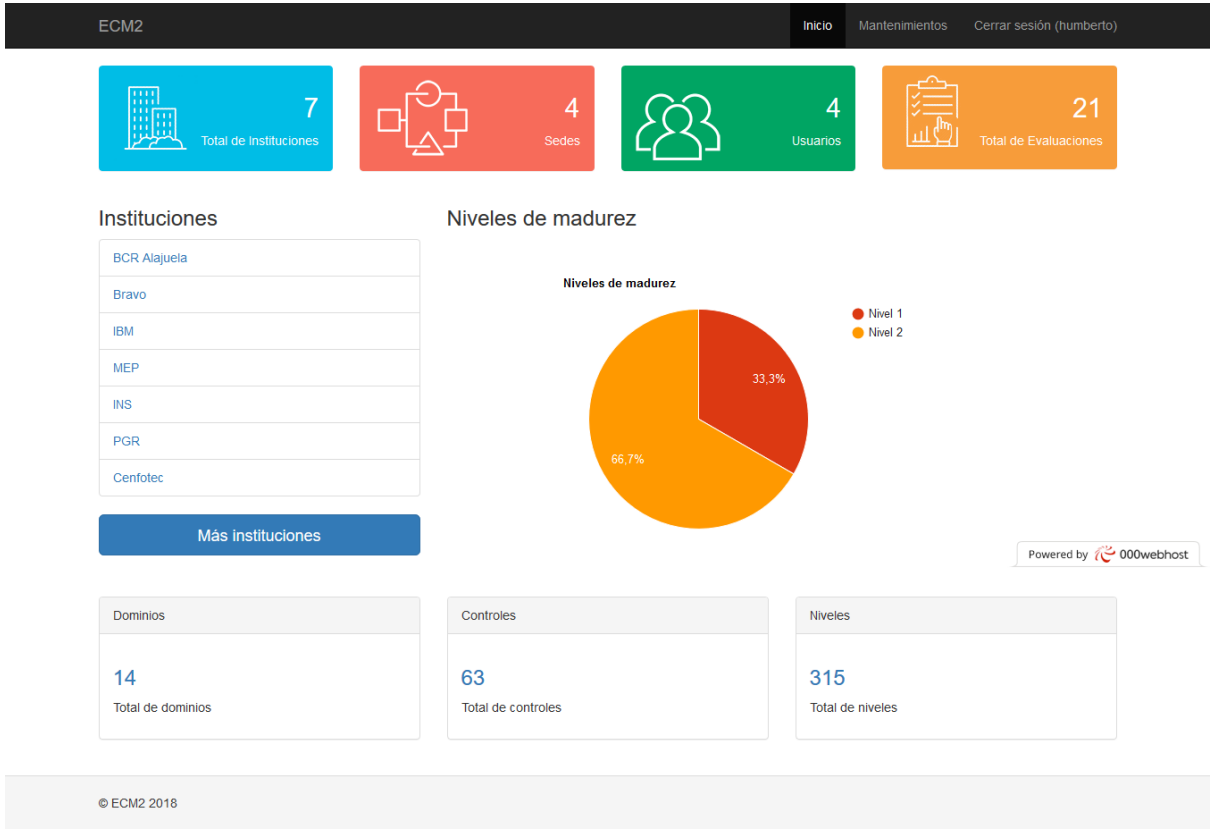


Cuando el usuario ingrese en su dispositivo, la tarjeta de firma digital, la aplicación detectará el certificado y el usuario podrá ingresar el número del PIN de la tarjeta. Una vez completado estos pasos y si el certificado se encuentra vigente, la aplicación permitirá el ingreso al panel de administración.



Panel de administración

El panel de administración es un “Dashboard”, donde el usuario administrador puede recibir información en tiempo real, sobre las diferentes evaluaciones realizadas por las instituciones inscritas en la plataforma, tanto nivel de institución, de sede o un ponderado global, del nivel de madurez según el modelo aplicado.



El panel de administración está compuesto por una serie de elementos, los cuales además de ser informativos permiten la interacción del usuario con la aplicación.

Widget instituciones

Este panel muestra una vista rápida del total de las instituciones inscritas en la aplicación. Además, este es un acceso directo al manteamiento, por lo cual al dar clic sobre el icono, la aplicación desplegará el catálogo de las mismas.

Widget sedes

Este *widget* muestra el total de las diferentes sedes que se han creado en la aplicación, para este total no se hace distinción entre instituciones.

Widget usuarios

Este panel muestra el total de usuarios activos en la aplicación, además es un acceso directo al mantenimiento de usuarios.

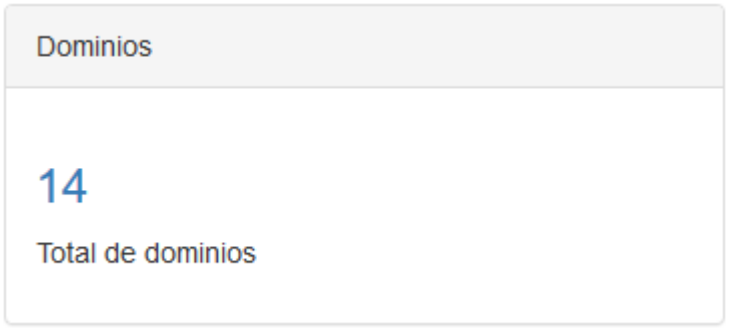
Widget evaluaciones

Este *widget* permite visualizar la cantidad total de evaluaciones, que se han realizado, este consolidado no hace distinción entre instituciones.

Al presionar el icono presente en el panel, la aplicación lo redireccionará a una página con el listado de todas las evaluaciones.

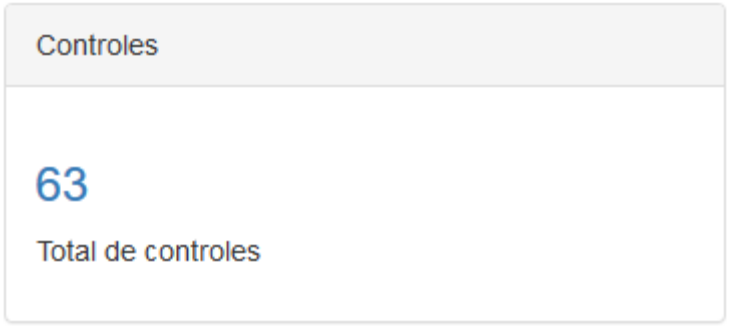
Widget dominios

Este se ubica en la parte inferior izquierda el panel de administración, en este la aplicación muestra el número total de dominios presentes en el modelo de madurez en Ciberseguridad ECM2. Además de ser un elemento informativo, este widget es un acceso directo al mantenimiento de dominios



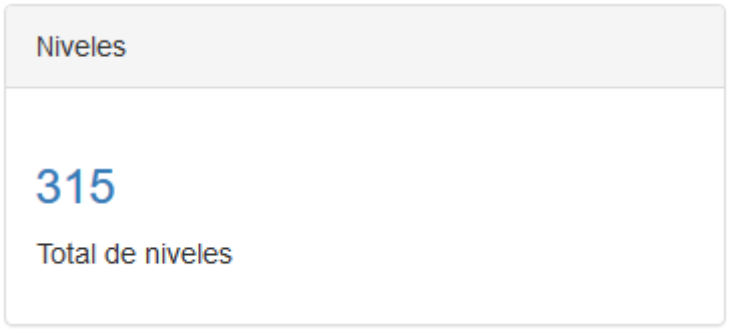
Widget controles

Este se encuentra en la parte inferior del panel de administración, este además de ser un acceso directo al mantenimiento de controles permite visualizar la cantidad de controles presentes en el modelo de madurez.



Widget Niveles

Este al igual que sus homólogos, permite visualizar la cantidad total de niveles, presentes en el modelo de Ciberseguridad ECM2. Asimismo, al presionar el enlace del numeral, traslada al usuario al mantenimiento de niveles.

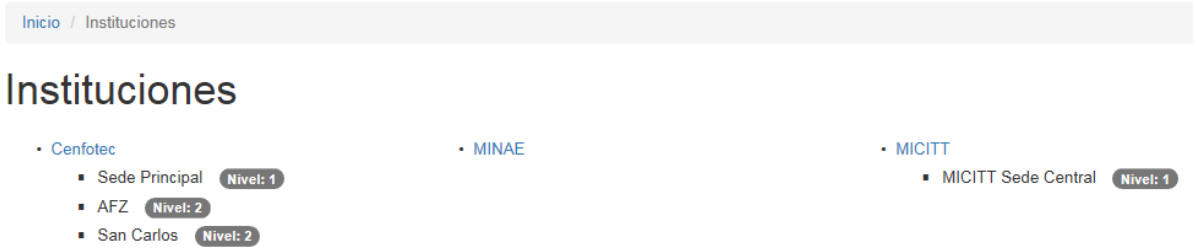


Barra lateral Instituciones

Esta se encuentra justo debajo de la primera línea de widgets, al lado izquierdo. En esta columna se ubican las últimas 10 instituciones inscritas en la aplicación. Tal listado además es un acceso directo a las evaluaciones de cada institución.

Botón más instituciones

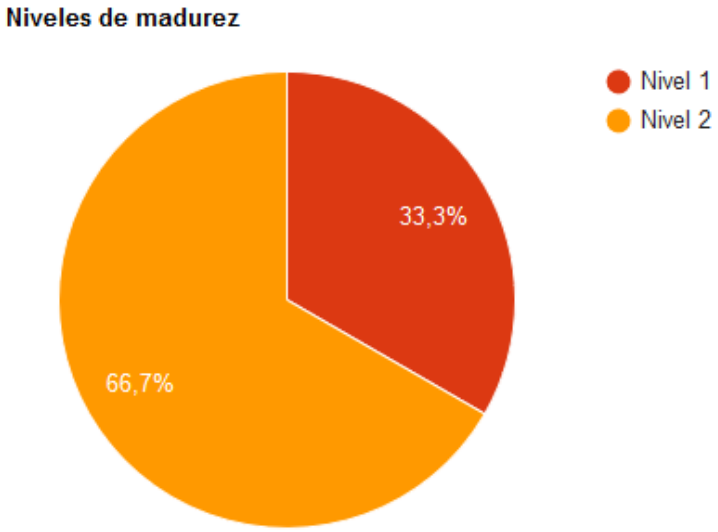
Al presionar el botón más instituciones presente en la barra lateral, la aplicación lo redirige al listado total de instituciones registradas.



Además del catálogo de instituciones el usuario puede observar las diferentes sedes pertenecientes a una institución, así como el nivel de madurez en ciberseguridad en que se encuentran según el modelo ECM2.

Widget resumen

Este se localiza en la zona central del panel de administración. Está conformado por un gráfico que muestra en tiempo real, el resumen de la situación global de todas las organizaciones evaluadas. Es decir, su lectura seria por ejemplo el X% de todas las instituciones evaluadas se encuentran en Y nivel

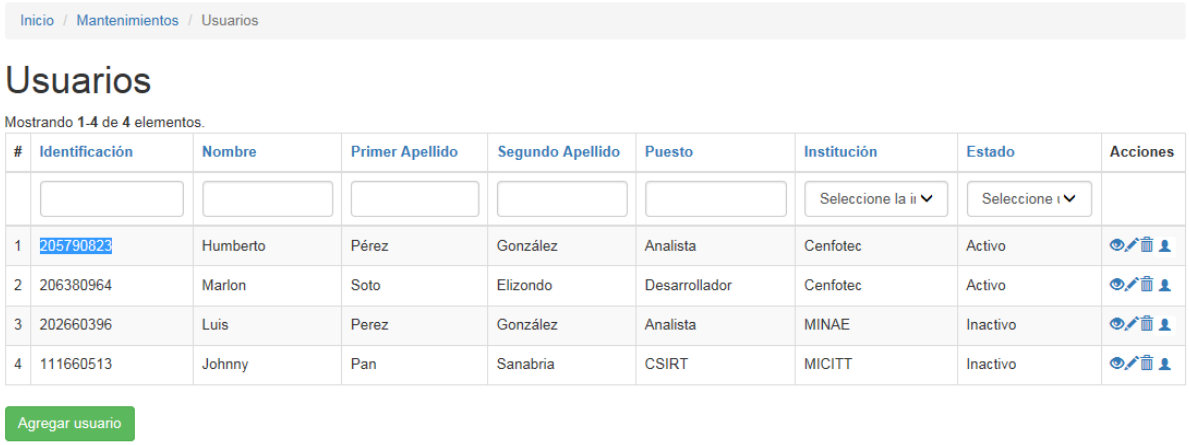


Menú mantenimientos

Este se ubica en la parte superior derecha sobre la barra de menú. Al presionar este ítem de menú, el usuario tiene acceso al catálogo de mantenimientos que alimentan la aplicación. Una vez ahí puede seleccionar el ítem de menú que mejor se adapte a sus necesidades.

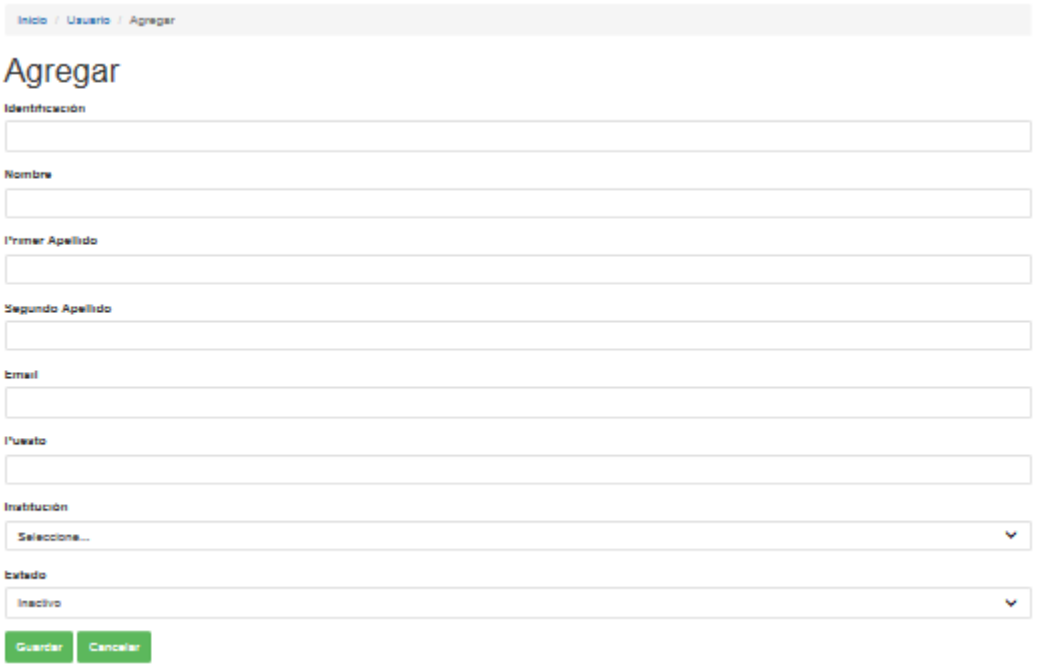
Mantenimiento de usuarios

Al seleccionar el ítem de menú usuarios, la aplicación muestra una tabla con los usuarios registrados en la aplicación, estos registros son mostrados independientemente de su condición (Activos/ Inactivos).



Agregar usuario

Para agregar un nuevo usuario, es necesario presionar el botón “Agregar usuario”, localizado en el mantenimiento. Una vez que se da clic sobre este botón, la aplicación presenta el siguiente formulario.



Al ingresar los datos es importante tomar en cuenta lo siguientes espacios requeridos:

a) Identificación
b) Nombre

c) Primer apellido
d) Email
e) Puesto
f) Institución

El formato del espacio Identificación debe ser numeral y este debe de coincidir con el número de cedula o DIMEX (Documento de identidad migratoria para extranjeros) en caso de los extranjeros. Solo son permitidos caracteres numéricos, no se deben incluir espacios o guiones el formato seria Ejemplo del formato 205790823.

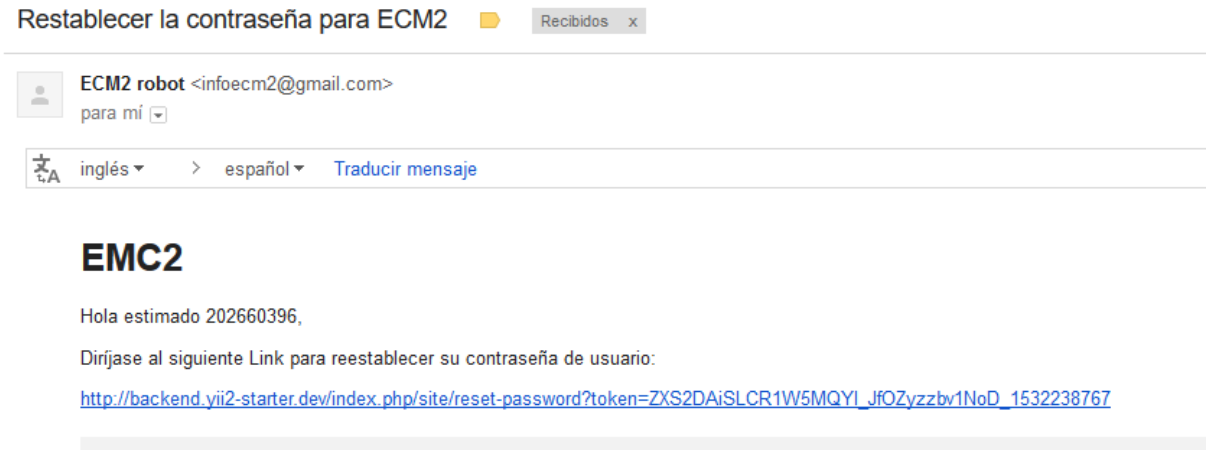
Cambiar estado a un usuario

Por defecto la aplicación crea el usuario inactivo, por ello para poder hacer uso de él, es necesario activarlo. Para cambiar el estado de un usuario es necesario ingresar al mantenimiento usuarios, en la lista de usuarios, localizar el registro que se desea activar y presionar el botón “Cambiar estado” ubicado en la columna “Acciones”

Una vez que el usuario presiona el botón, se muestra un nuevo formulario en donde se puede cambiar el estado a un determinado usuario (Activar/ Desactivar)

Cuando se realiza la operación activar, la aplicación envía un correo electrónico al usuario para que este puede ingresar a la aplicación y personalizar sus credenciales y continuar haciendo uso de esta.

Para ingresar el usuario debe presionar el enlace incluido en el cuerpo del correo electrónico.

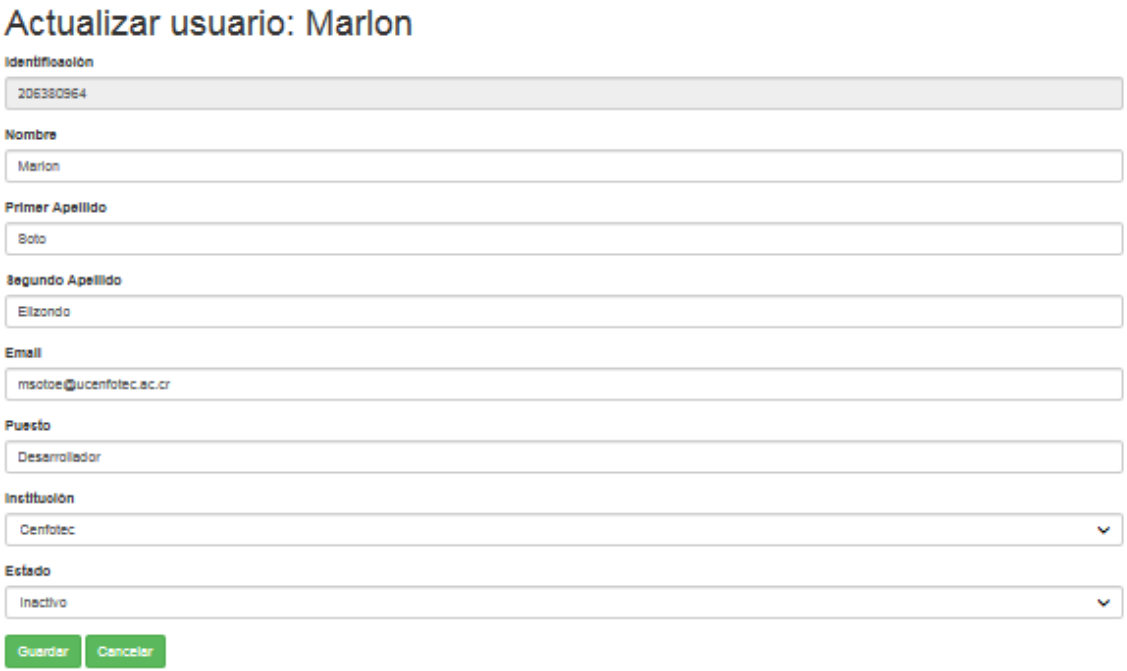


El enlace del correo electrónico tiene una vida útil de una hora por ello es importante que en caso de una no activación, se comunique con el administrador de la plataforma con el fin de que pueda generar otro enlace.

Actualizar usuario

Para actualizar un usuario es necesario ingresar al menú mantenimientos de usuarios, y dar clic sobre el botón “Actualizar” ubicado en la columna acciones (Icono del lápiz)

Una vez realizada la acción se muestra un formulario con los datos del usuario previamente ingresados. Es importante mencionar que todos los valores a excepción de la identificación pueden ser actualizados por el usuario.

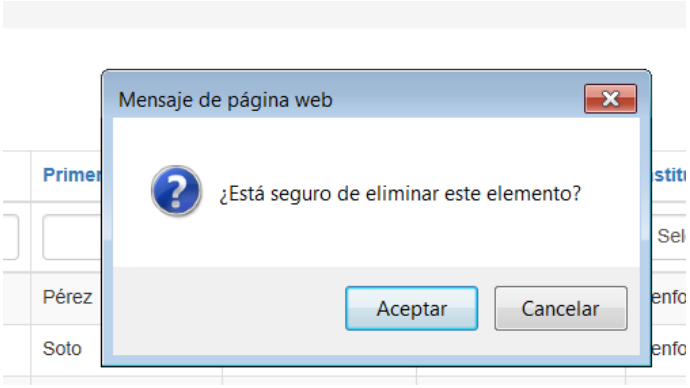


Para guardar los nuevos valores, el usuario debe dar clic sobre el botón “Guardar”; asimismo, si no desea realizar ningún cambio, puede presionar el botón Cancelar y mantener los datos sin variación.

Eliminar usuario

Para eliminar un usuario, es necesario ingresar al menú mantenimientos de usuarios, seleccionar un registro y dar clic sobre el botón “Eliminar” ubicado en la columna acciones (Icono de cesto de basura).

Una vez que usuario oprime dicho botón, el sistema lanzará un mensaje de corroboración con el fin de verificar si realmente el usuario desea ejecutar dicha acción. En caso de que desee proseguir, debe presionar el botón “Aceptar”, por el contrario, si quiere anular la operación, debe presionar el botón “Cancelar”.

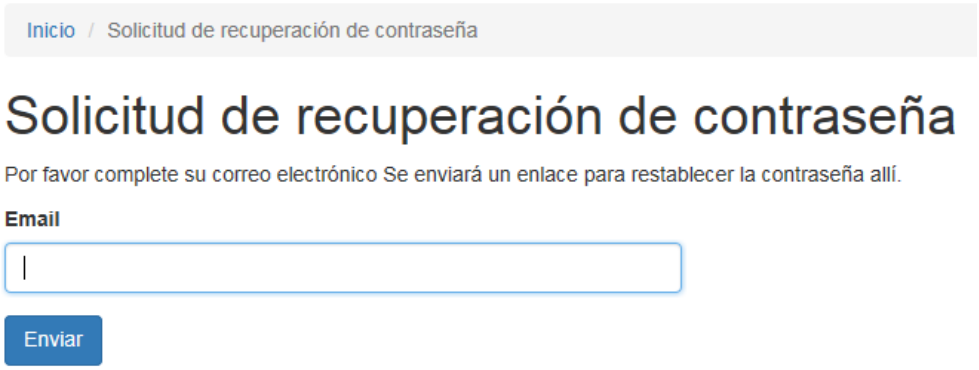


Si el registro no cuenta con datos asociados a él, se eliminará; en caso contrario, el sistema le mostrará un mensaje con el motivo por el cual no pudo llevar a cabo la operación.

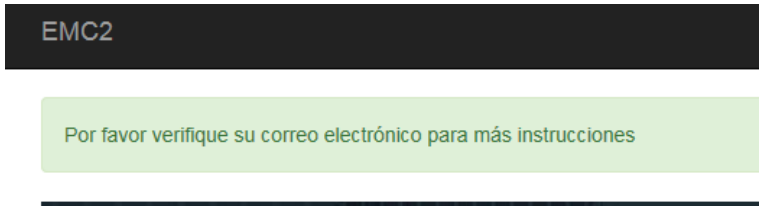
Recuperar contraseña

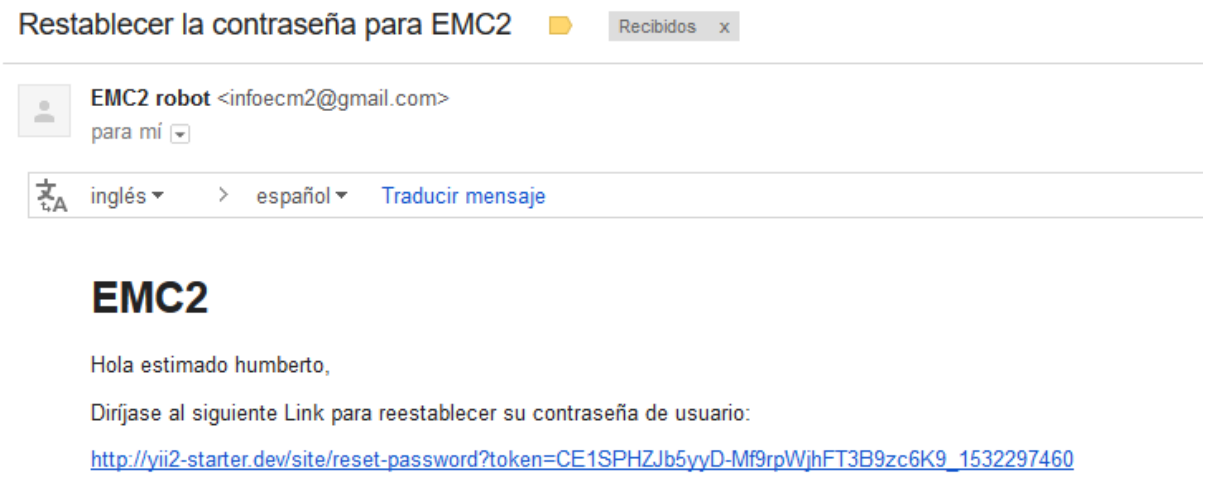
En caso de que el usuario olvide su contraseña, el sistema provee la posibilidad de restablecerla, para eso debe presionar el enlace que aparece en la sección de Iniciar sesión por medio de usuario y contraseña.

Una vez que presione el enlace, se le mostrará un formulario donde debe agregar el correo electrónico con que se registró en el sistema y presionar el botón enviar.



Cuando se lleve a cabo esta acción, la aplicación le mostrará que las instrucciones de como proseguir. Además, se le enviará un correo con un enlace para restablecer la contraseña.



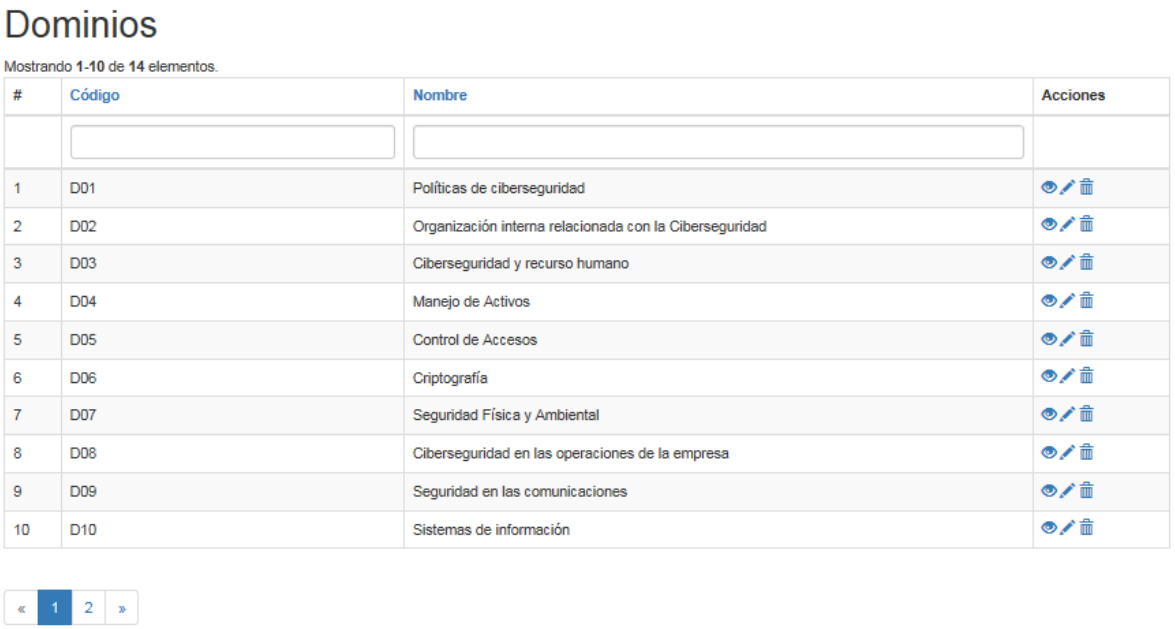


Mantenimiento dominios

Para ingresar al mantenimiento Dominios, se puede hacer de dos maneras:

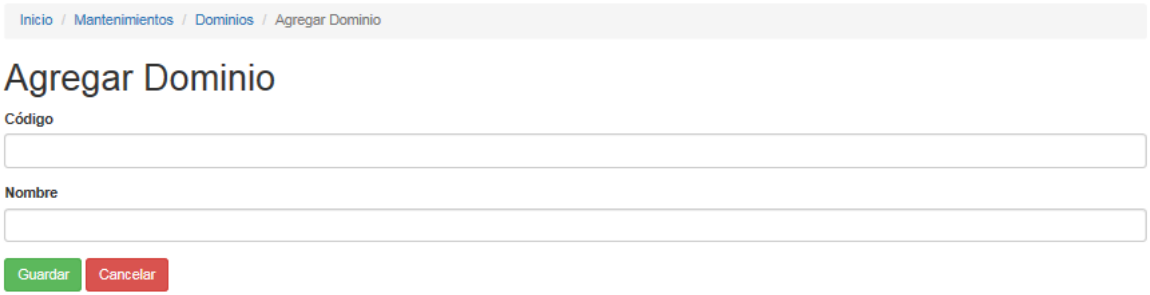
a) Mediante el widget Dominios, ubicado en el panel de administración.
b) Por medio del menú Mantenimiento, ítem de menú Dominios

Al seleccionar el ítem de menú Dominios, la aplicación le muestra una tabla con los Dominios registrados. Al igual que en el mantenimiento de usuarios sobre esta tabla se pueden realizar una seria de operaciones que posteriormente se van a ir detallando.



Agregar dominio

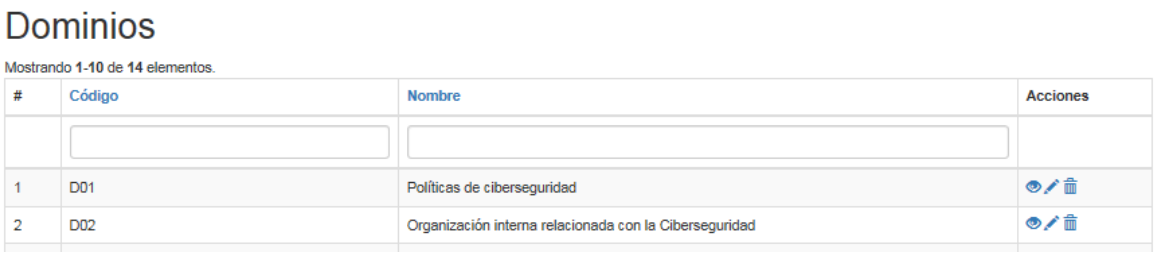
Para agregar un nuevo dominio es necesario presionar el botón “Agregar dominio”, localizado en el mantenimiento. Una vez que se da clic sobre este botón, la aplicación le presenta el siguiente formulario.



Los espacios Código y Nombre son espacios requeridos. En caso que el usuario desee desistir de la operación este puede presionar el botón “Cancelar”, y anular la transacción.

Actualizar dominio

Para actualizar un Dominio, es necesario ingresar al menú mantenimientos de Dominios, y dar clic sobre el botón “Actualizar” ubicado en la columna Acciones (Icono del lápiz)

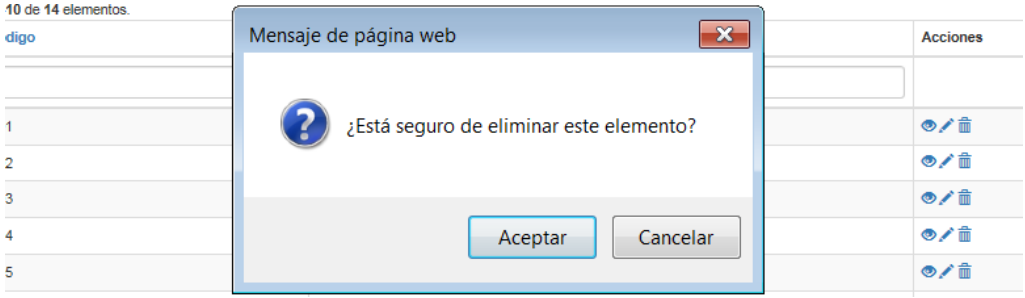


Una vez realizada la acción, se muestra un formulario con los datos del Dominio previamente ingresados. Estos pueden ser actualizados por los nuevos valores, una vez que el usuario presione el botón “Guardar”

Eliminar dominio

Para eliminar un Dominio es necesario ingresar al menú mantenimientos de Dominios, seleccionar un registro y dar clic sobre el botón “Eliminar” ubicado en la columna acciones (Icono de cesto de basura).

Una vez que usuario oprime dicho botón, el sistema lanzará un mensaje de corroboración con el fin de verificar si realmente desea ejecutar dicha acción. Si se desea proseguir, se tiene que presionar el botón “Aceptar”; por el contrario, si quiere anular la operación, debe presionar el botón “Cancelar”.



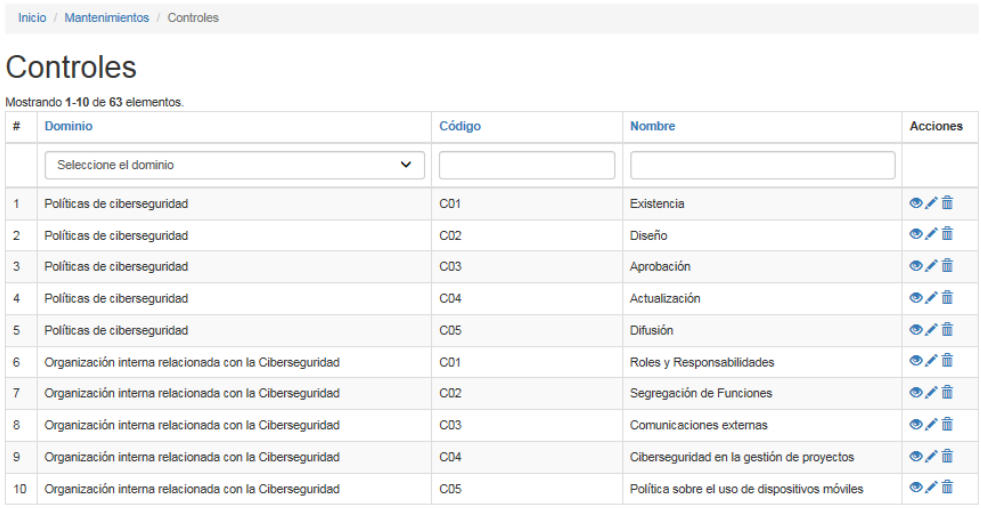
En caso que el Dominio posea datos asociados a él, no se podrá eliminar, y la aplicación le mostrará un mensaje con el motivo por el cual no se pudo completar la operación.

Mantenimiento Controles

Para hacer ingreso al mantenimiento Controles, existen dos maneras:

a) Mediante el widget Controles, ubicado en el panel de administración.
b) Por medio del menú Mantenimiento, ítem de menú Controles

Una vez que el usuario selecciona el menú controles, la aplicación muestra una tabla con los controles ingresados a la aplicación.



Agregar control

Para agregar un nuevo control, es necesario presionar el botón “Agregar control”, ubicado en el mantenimiento. Una vez que se da clic sobre este botón, la aplicación presenta el siguiente formulario.

Una vez ahí, es necesario completar los todos los espacios y presionar el botón “Guardar”.

Es importante mencionar que en caso de un faltante el sistema alertará sobre los espacios requeridos.

Actualizar control

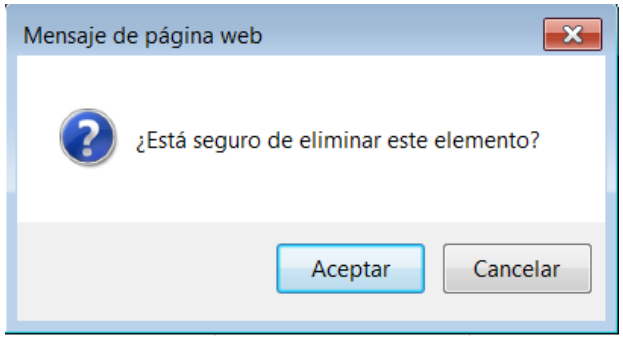
Para actualizar un Control, es necesario ingresar al menú mantenimientos de Controles, y dar clic sobre el botón “Actualizar” ubicado en la columna acciones (Icono del lápiz)

Una vez que se realiza esta acción, el sistema le desplegará un formulario con los datos ingresados anteriormente. Estos pueden ser sobrescritos por los nuevos valores que el usuario desea y salvados al presionar el botón “Guardar”.

Eliminar un control

Para eliminar un Control, es necesario ingresar al menú mantenimientos de Controles, seleccionar un registro y dar clic sobre el botón “Eliminar” ubicado en la columna acciones (Icono de cesto de basura).

Una vez que usuario oprime dicho botón, el sistema lanzará un mensaje de corroboración, con el fin de verificar si realmente el usuario desea ejecutar dicha acción. En caso de que desee proseguir debe presionar el botón “Aceptar”; por el contrario, si quiere anular la operación, debe presionar el botón “Cancelar”.



Si el control no está siendo utilizado por un nivel o una evaluación, este será eliminado, en caso de encontrarse en uso, la aplicación mostrara la advertencia de porque no fue posible eliminar.

Mantenimiento Niveles

Para hacer ingreso al mantenimiento de Niveles, existen dos maneras:

a) Mediante el widget Niveles, ubicado en el panel de administración.
b) Por medio del menú Mantenimiento, ítem de menú Niveles

Una vez que el usuario presiona cualquiera de las dos alternativas antes mencionadas, la aplicación mostrará la siguiente pantalla.

Agregar un nivel

Para agregar un nuevo nivel a la aplicación, es necesario presionar el botón “Agregar nivel”, localizado en el mantenimiento del mismo nombre.

Una vez que el usuario realiza esta acción, aparecerá el siguiente formulario:

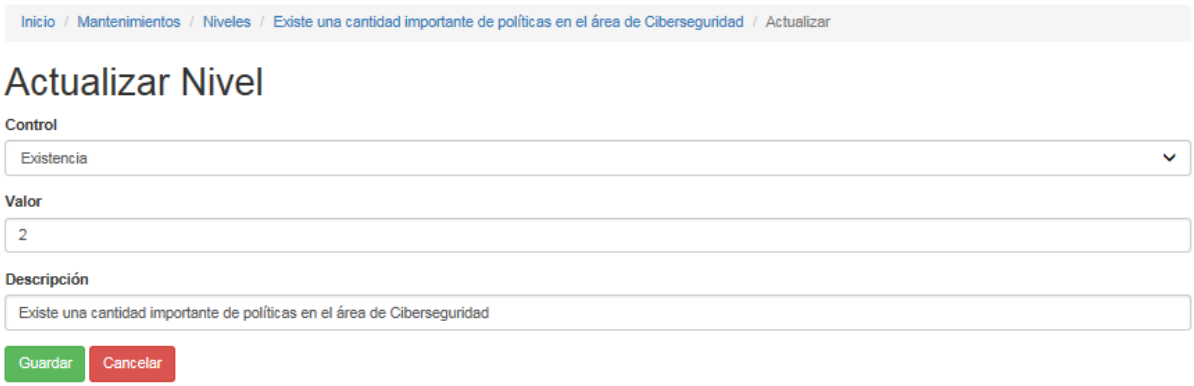
Para este es necesario completar todos los espacios y seleccionar el control al cual pertenece, de lo contrario, la aplicación brindará retroalimentación sobre los espacios faltantes. Una vez completado el formulario, es necesario dar clic sobre el botón guardar, y el nuevo nivel estará disponible.

Actualizar nivel

Para actualizar nivel es necesario que el usuario seleccione un registro de la tabla mantenimiento niveles y presionar el botón “Actualizar” (Icono de lápiz), ubicado en la columna acciones.

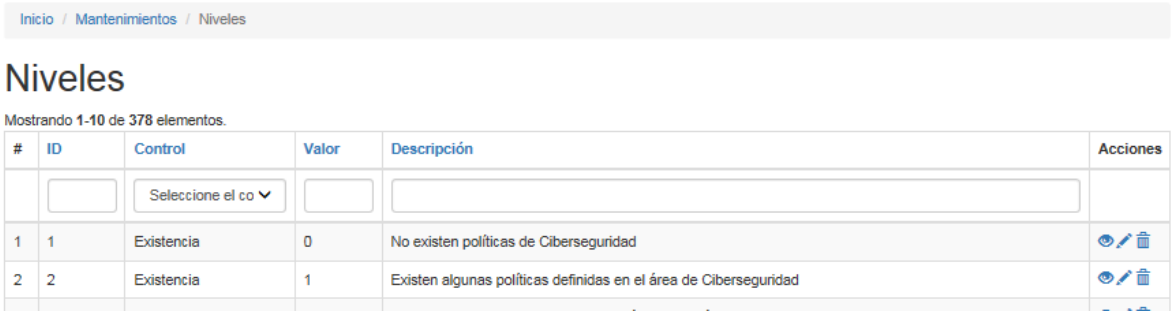
Una vez que el usuario presiona ese botón, aparecerá un formulario con la información del nivel que se desea editar.

Es importante señalar que al igual que el apartado de ingresar nivel, todos los espacios son necesarios por ello no es válido eliminar el contenido de ninguna opción. Una vez que se realiza la edición de los espacios deseados, se debe dar oprimir el botón “Guardar” para salvar los cambios.



Eliminar nivel

Para eliminar un nivel es necesario que el usuario seleccione un registro dentro de la tabla de niveles ubicada en el mantenimiento, y de clic sobre el botón “Eliminar”, ubicado en la columna acciones (Icono de cesto de basura).



Cuando se oprime el botón eliminar, aparecerá un mensaje en el cual el usuario debe confirmar que desea llevar a cabo dicha acción; en caso que la respuesta sea afirmativa y que el nivel no se encuentre asociado con una evaluación, el nivel será eliminado. Caso contrario la aplicación señalará el motivo por el cual no se pudo completar la acción.

Mantenimiento Instituciones

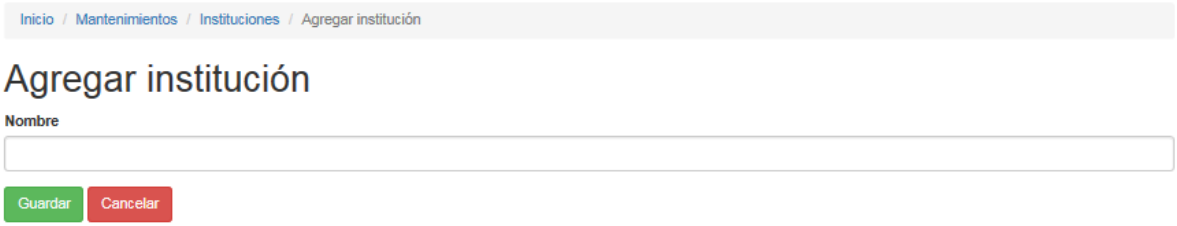
Para hacer ingreso al mantenimiento instituciones, el usuario tiene con dos opciones.

a) Mediante el widget Instituciones, ubicado en el panel de administración.
b) Por medio del menú Mantenimiento, ítem de menú Instituciones

Una vez que se elige alguna de estas alternativas el usuario ingresará a la pantalla mantenimientos en donde podrá visualizar todas las instituciones registradas en la aplicación.

Agregar institución

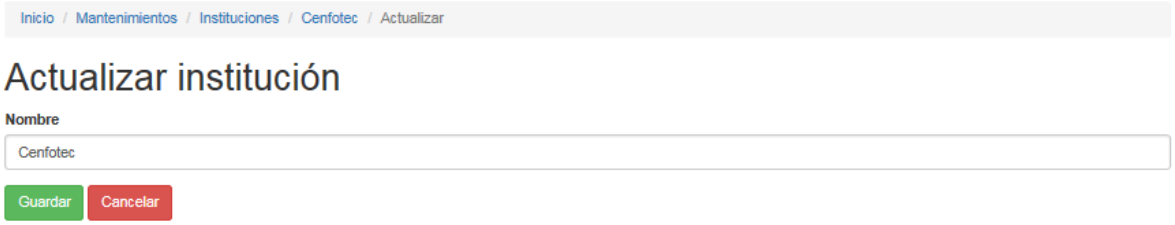
Para agregar una institución, es necesario dar clic en el botón “Agregar Institución”, localizado en el mantenimiento instituciones. Una vez realizada esta acción, aparecerá un formulario en la cual el usuario podrá ingresar los datos de la nueva institución que desea agregar.



Actualizar institución

Para actualizar una institución, es necesario que el usuario seleccione un registro de la tabla mantenimiento y presione el botón “Actualizar” (Icono de lápiz), ubicado en la columna acciones.

Una vez que el usuario presiona ese botón, aparecerá un formulario con la información que se desea editar.



Para salvar los cambios, solo es necesario oprimir el botón “Guardar”, o “Cancelar” en caso de que se desee anular la acción.

Eliminar institución

Para eliminar una institución, es necesario que el usuario seleccione un registro dentro de la tabla de ubicada en el mantenimiento y dé clic sobre el botón “Eliminar”, ubicado en la columna acciones (Icono de cesto de basura).

Cuando se oprime el botón eliminar, aparecerá un mensaje en el cual el usuario debe confirmar que desea llevar a cabo la acción; en caso que la respuesta sea afirmativa y que la institución no se encuentre asociado con una evaluación, el registro será eliminado. Caso contrario, la aplicación señalará el motivo por el cual no se pudo completar.

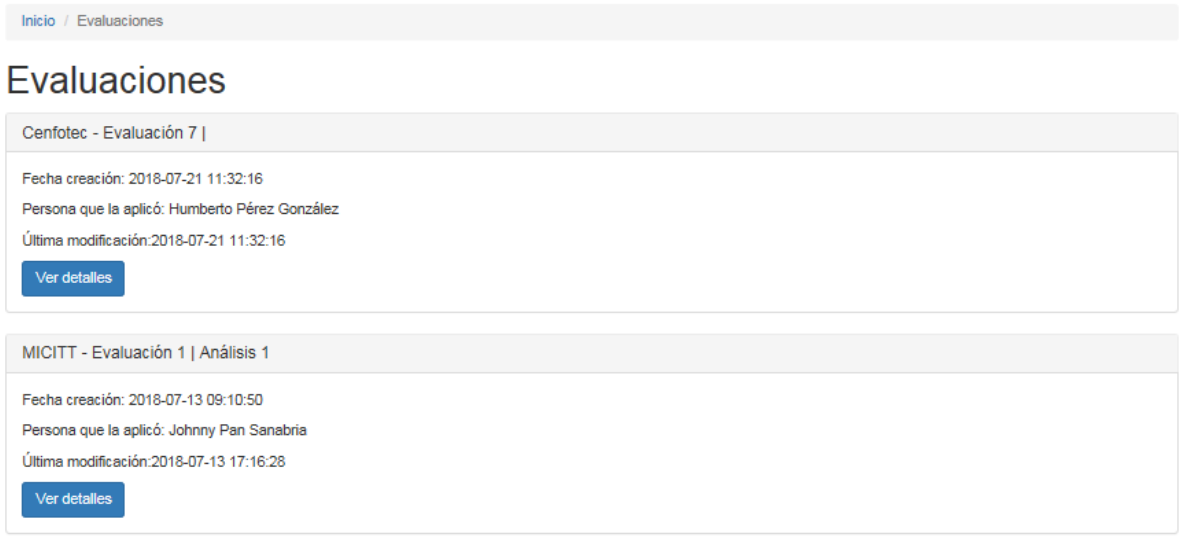
Mantenimiento Accesos y permisos

Cuando se crea y activa un usuario en la aplicación, este por defecto es creado bajo el perfil de usuario externo, lo que significa que este puede acceder a la sección de la aplicación donde se pueden aplicar y consultar evaluaciones, para una institución en particular. En caso de que se desee otorgar cambiar el rol a un usuario administrador esto se puede hacer por medio del mantenimiento Accesos y permisos, ubicado en el menú Mantenimientos.

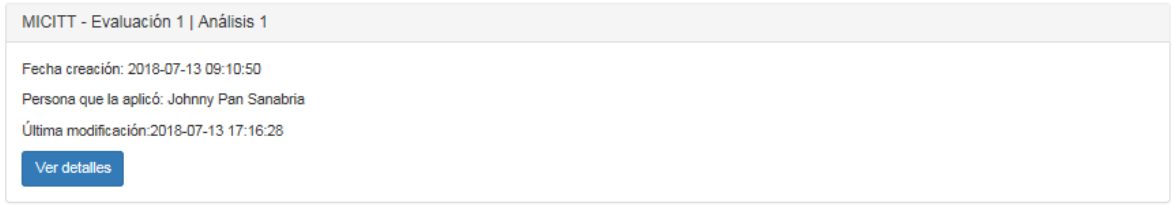
Una vez ahí, la aplicación mostrar la lista de los usuarios registrador en la aplicación, y adicionalmente un botón ver (Icono celeste). Si el usuario presiona este botón la aplicación lo dirigirá a la sección de asignación, donde se puede agregar o remover un rol para el registro seleccionado.

Ver evaluaciones

Al presionar el widget Evaluaciones, ubicado en el panel de administración, la aplicación mostrará el listado de todas las evaluaciones realizadas sin importar la institución o sede a la que pertenezcan.



En la lista de evaluaciones, cada panel o caja representan, una evaluación, la cual está conformada de la siguiente manera:



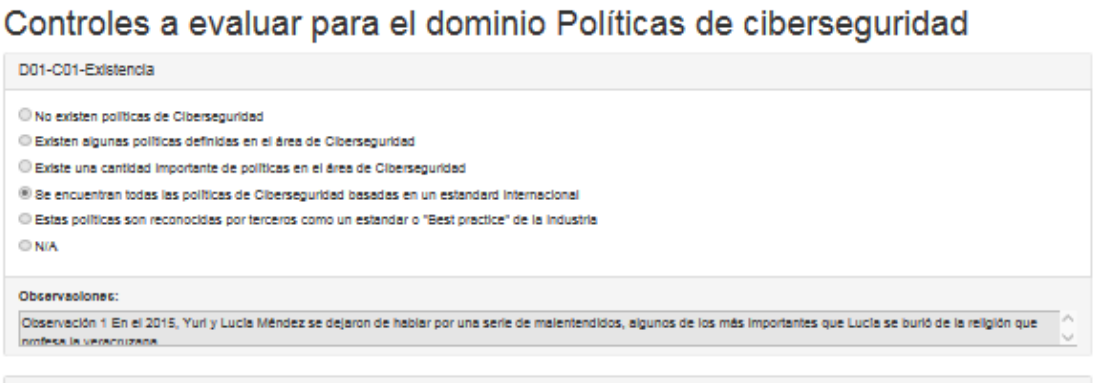
- Encabezado de la caja: lo conforman el nombre de la institución donde se realizó la evaluación, seguido de una descripción o comentario emitido por el usuario.
- Fecha de creación: es la fecha cuando la evaluación fue creada, no necesariamente es la misma fecha de finalización.
- El nombre de la persona responsable de aplicar la evaluación.
- Fecha de la última modificación.
- Un botón en el cual, si se presiona se puede visualizar en detalle la evaluación, y sus respectivas notas, por dominio y global.

Botón Ver detalles evaluación

Al presionar el botón ver detalles ubicado en el panel de la evaluación, se mostrará el resumen de la evaluación. Tal y como se muestra a continuación.

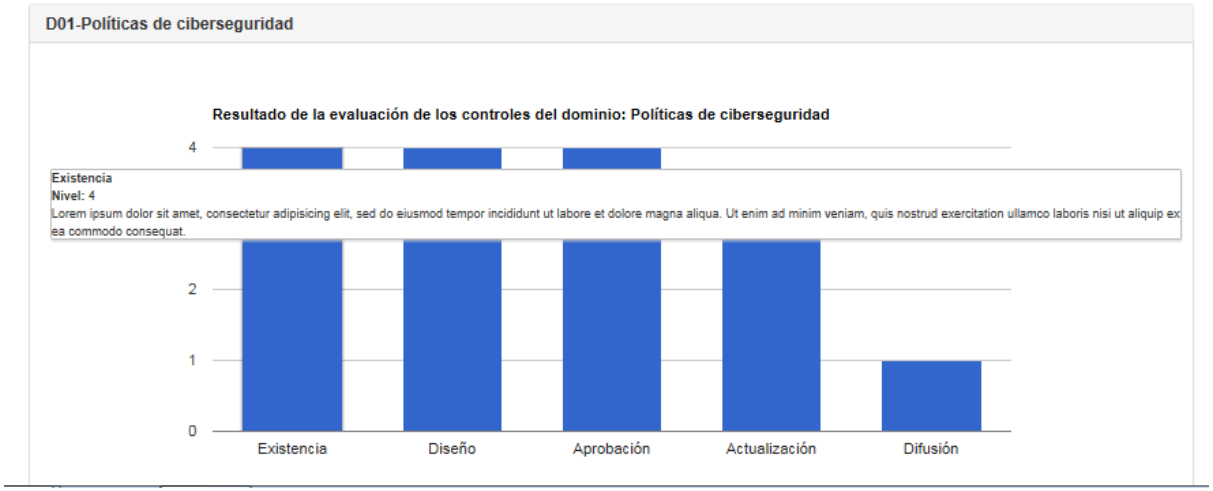
Esta vista está compuesta por los dominios que componen el modelo, y nota que recibieron al confeccionar la evaluación. Además de un gráfico que muestra el comportamiento de cada control.

Adicionalmente, en el panel se ubica otro botón, el cual muestra los datos que ingreso el usuario y que produjeron dicha nota.



Gráficos por dominio

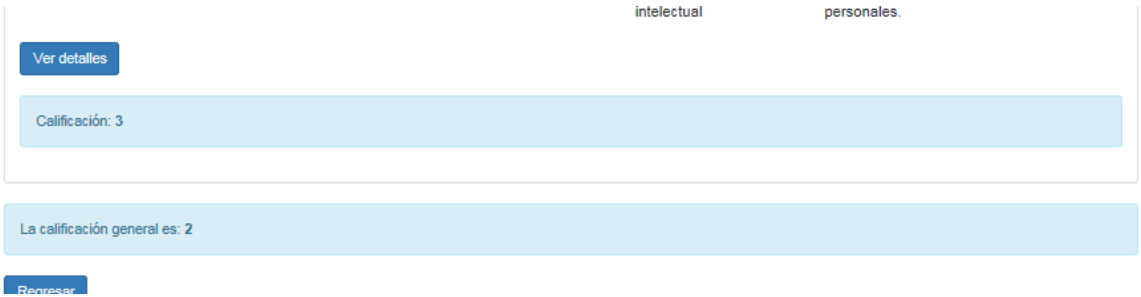
Los gráficos son una representación visual de las respuestas que emite el usuario; en estos aparecen reflejados la calificación otorgada a cada control, así como las observaciones en caso de tenerlas. Esta se puede ver al pasar el cursor sobre cada barra del gráfico.



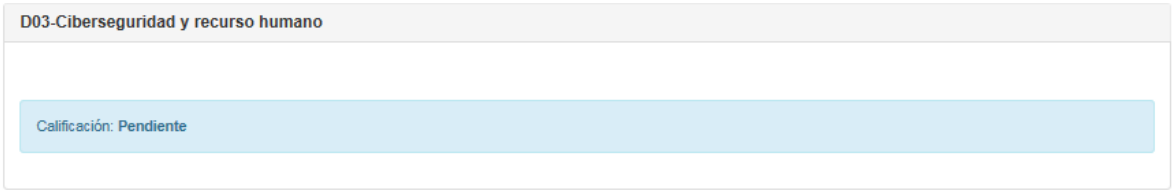
¿Cómo funcionan las notas?

Debido a que en seguridad se toma como un referente el principio de que “una cadena es tan fuerte como su eslabón más débil”, entonces se toma como calificación para el dominio la nota más baja obtenida por los controles, asimismo para la nota global de la evaluación se mantiene este mismo concepto, por ello la nota estará dada por la menor calificación de los dominios.

Dicha nota aparece al pie de la evaluación, después de los paneles de dominios.

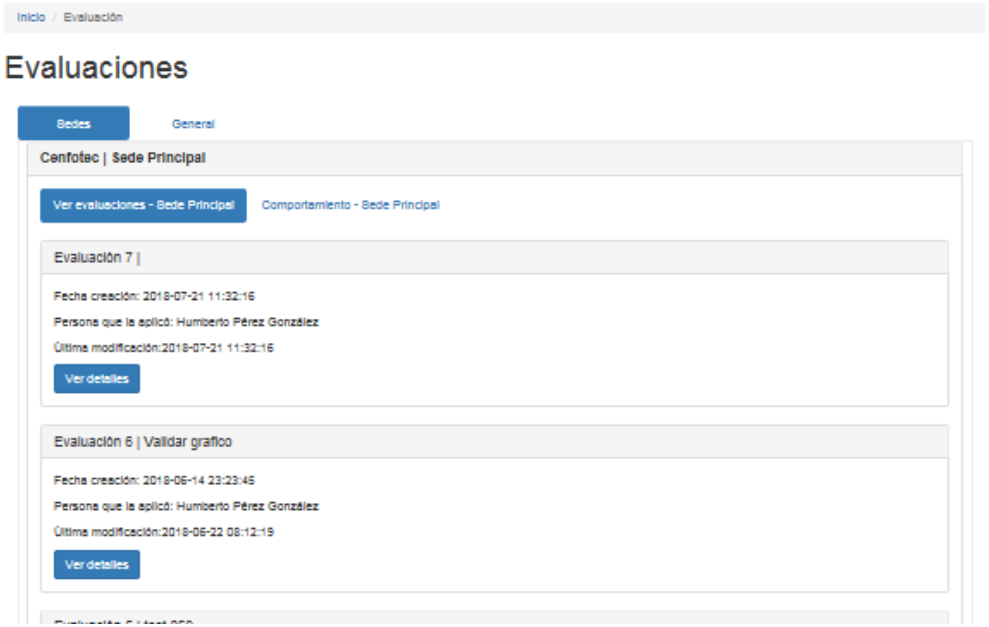


Cuando el usuario aún se encuentra completando la evaluación, o la dejó inconclusa, la caja del dominio sin evaluar mostrara la leyenda “Pendiente” en la calificación.

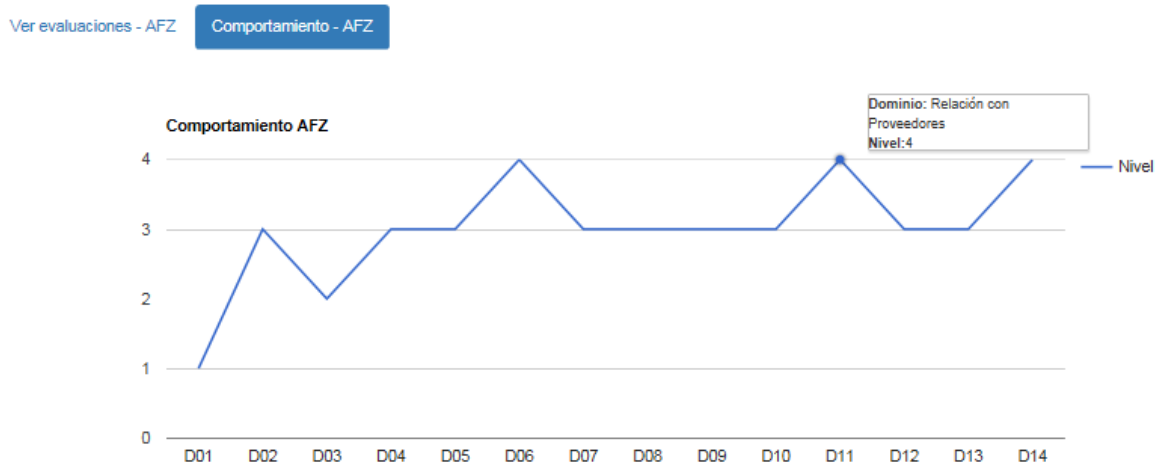


Evaluaciones por institución

Al hacer clic sobre las instituciones presentes en la barra lateral, del panel de admiración o en la lista general de instituciones, aparecerá una pantalla con las evaluaciones para una institución en particular. Estas evaluaciones están ordenadas por sede; asimismo, dentro del panel de sede están ordenadas de la más reciente a la más antigua, tal y como se muestra en la siguiente gráfica.



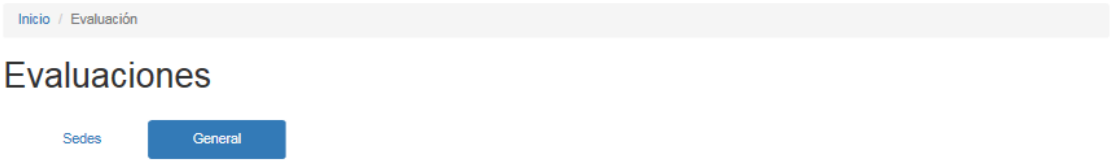
Dentro del panel de cada sede van a existir dos pestañas, las cuales muestran las evaluaciones, con el formato que se explicó anteriormente y el “Comportamiento por sede”, en donde se muestra el gráfico de la última evaluación realizada.



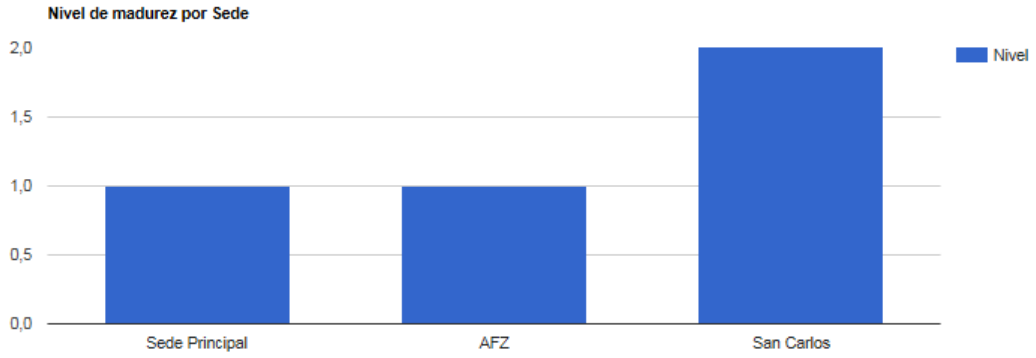
Es importante resaltar que dicho grafico se genera en tiempo real por lo cual en caso de tener dominios pendientes que evaluar este, aún se mostrará.

Gráficos comportamiento general por institución

Cuando se selecciona una institución, se muestra en una pestaña la lista con las evaluaciones, ordenadas por sede, tal y como se mencionó con anterioridad y en la otra pestaña la vista general con el resumen de los comportamientos.



En la pestaña general aparecerán los siguientes gráficos



Esta muestra una comparativa del nivel de madurez en que se encuentran las sedes, según el modelo ECM2. En caso de que una sede no cuente con la evaluación completa aparecerá la nota parcial.

Gráfico comparación de comportamientos

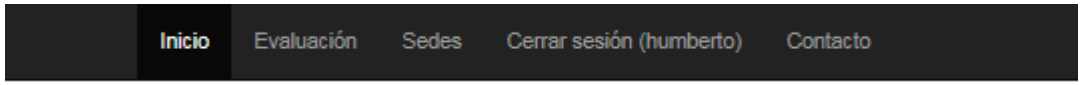
Cuando una institución cuenta con más de una sede, el usuario tiene la posibilidad de ver una comparativa del desempeño de cada sede, con el fin de valorar las posibles acciones a seguir y si es necesario aplicar una medida correctiva o compartir conocimiento entre las sedes.

No se puede mostrar el comportamiento para **Sede Principal** , por que la evaluación se encuentra incompleta .

Para la construcción de este gráfico, es necesario que la evaluación de cada sede se encuentre completa, caso contrario aparecerá un mensaje del porqué de la exclusión.

Crear una evaluación

Cuando un usuario con el rol externo, inicia sesión en la aplicación tal y como se ha explicado anteriormente, el sistema le muestra el siguiente menú



Al presionar el ítem evaluaciones, el sistema le muestra al usuario el listado de las evaluaciones existentes, en caso de tenerlas ordenadas por sede y el botón crear una evaluación.

Una vez que el usuario da clic sobre el botón, la aplicación le muestra la siguiente pantalla:

En donde el usuario debe seleccionar la sede a la cual va aplicar la evaluación y una breve descripción o comentario sobre la misma.

Una vez que completa dichos espacios y presiona “Crear evaluación”, la evaluación esta lista para ser aplicada.

EMC2

Inicio Evaluación Sedes Cerrar sesión (humberto) Contacto

Inicio / Evaluaciones / Dominios evaluados

Dominios evaluados

Evaluación: Centotec | Sede Principal - 7
Fecha: 2018-07-23 17:16:50
Descripción: Esto es una prueba par el manuel de usuario
Fecha de modificación: 2018-07-23 17:16:50

D01-Políticas de ciberseguridad

Evaluar

Calificación: **Pendiente**

D02-Organización interna relacionada con la Ciberseguridad

Evaluar

Calificación: **Pendiente**

D03-Ciberseguridad y recurso humano

Evaluar

Calificación: **Pendiente**

D04-Manejo de Activos

Evaluar

Calificación: **Pendiente**

D05-Control de Accesos

Evaluar

Calificación: **Pendiente**

D06-Criptografía

Evaluar

Calificación: **Pendiente**

D07-Seguridad Física y Ambiental

Evaluar

Calificación: **Pendiente**

D08-Ciberseguridad en las operaciones de la empresa

Evaluar

Calificación: **Pendiente**

D09-Seguridad en las comunicaciones

Evaluar

Calificación: **Pendiente**

D10-Sistemas de información

Evaluar

Calificación: **Pendiente**

D11-Relación con Proveedores

Evaluar

Calificación: **Pendiente**

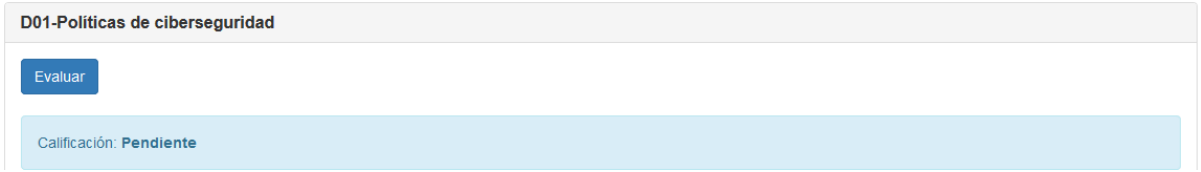
D12-Gestión de incidentes de Ciberseguridad

Evaluar

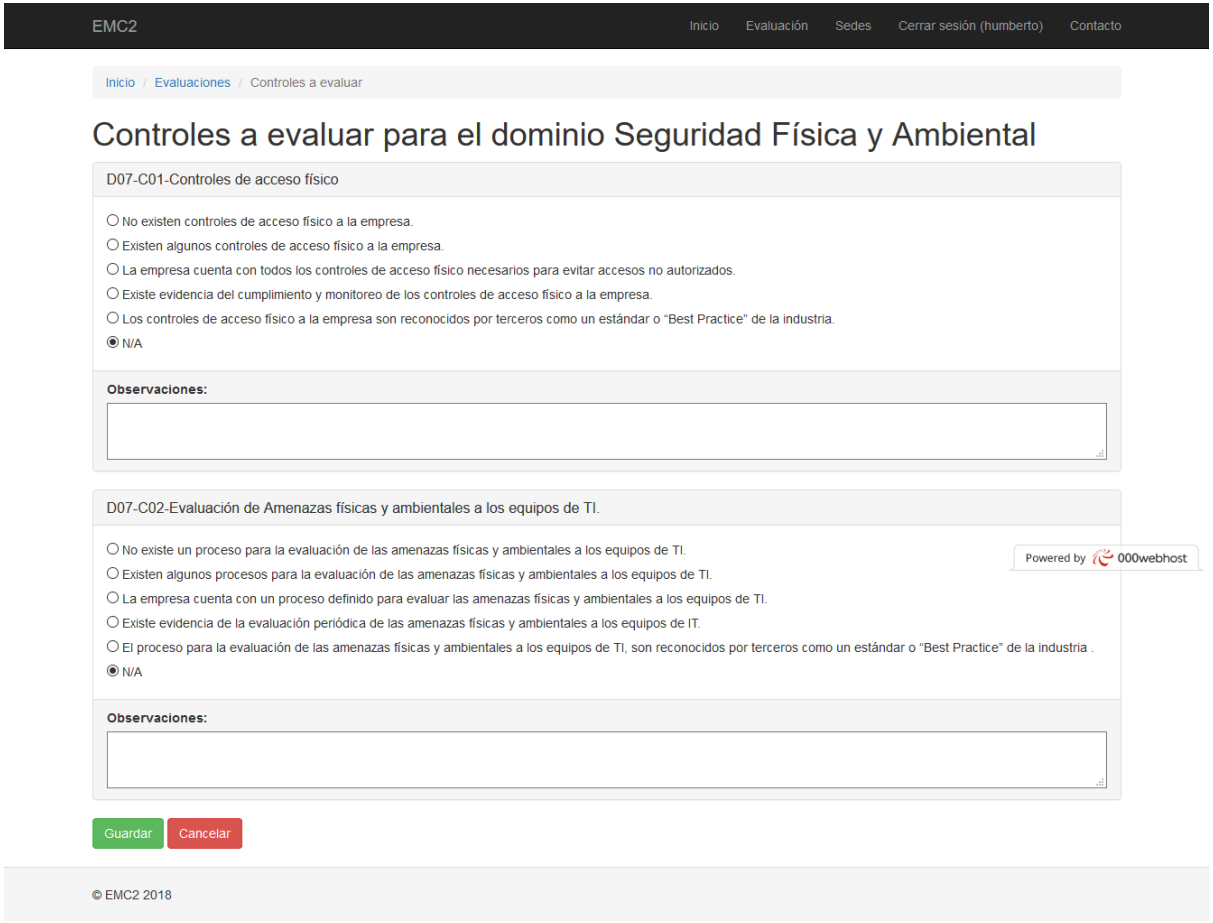
Calificación: **Pendiente**

D13-Continuidad del Negocio

Para evaluar un dominio es necesario que el usuario presione el botón “Evaluar”; una vez hecho esto, aparecerán una serie de preguntas de selección con la evaluación de los controles.



En caso de que un control no aplique para la sede, la aplicación dispone de una opción y este no será tomado en cuenta en la nota del dominio ni en la evaluación global. Asimismo, si el usuario considera necesario incluir un comentario en una pregunta, lo puede realizar en el espacio, observaciones.



Una vez que el usuario presiona el boton “Guardar”, la evaluación del dominio será salvada y se retornará a la página donde se encuentran todos los dominios, para repetir el proceso y evaluar otro dominio.

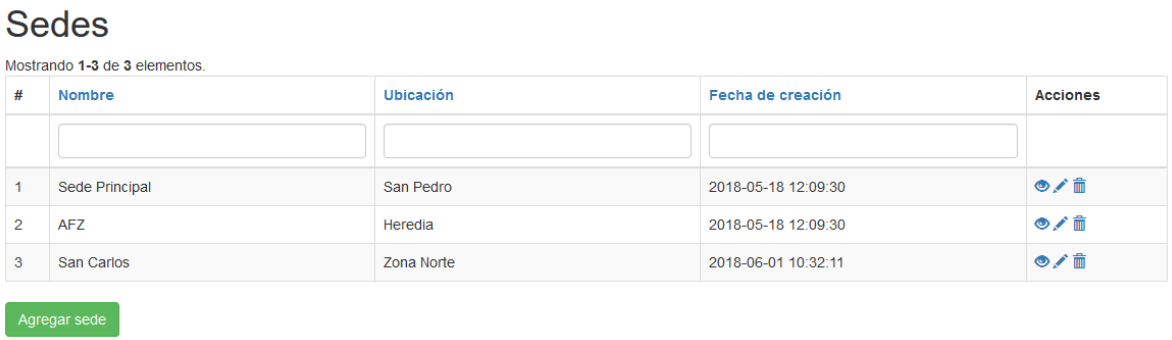
Actualizar una evaluación

Un usuario puede editar una evaluación en cualquier momento; para esto es necesario ingresar al listado de evaluaciones mediante el ítem de menú “Evaluaciones”; una vez ahí elige la que desea editar y presiona el botón “Ver detalles”, que lo llevará a la pantalla de dominios a evaluar, ahí puede continuar evaluando los dominios faltantes, o editar respuestas anteriormente ingresadas al presionar el botón “Ver detalles”

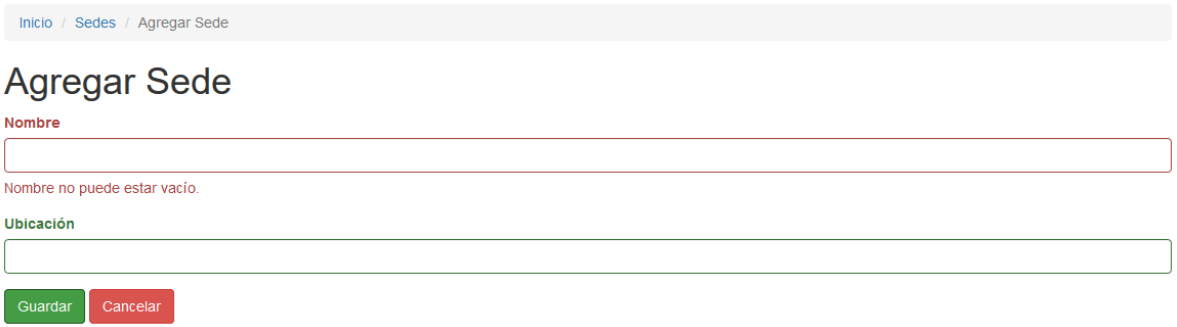
Una vez dentro del formulario de preguntas, solo se debe guardar la información con los nuevos datos editados.

Mantenimiento sedes

Cuando se crea una institución por defecto se crea una sede, sin embargo, en caso que una organización requiera adicionales, el usuario tiene la posibilidad de crearlas de una manera sencilla, por medio del menú Sedes



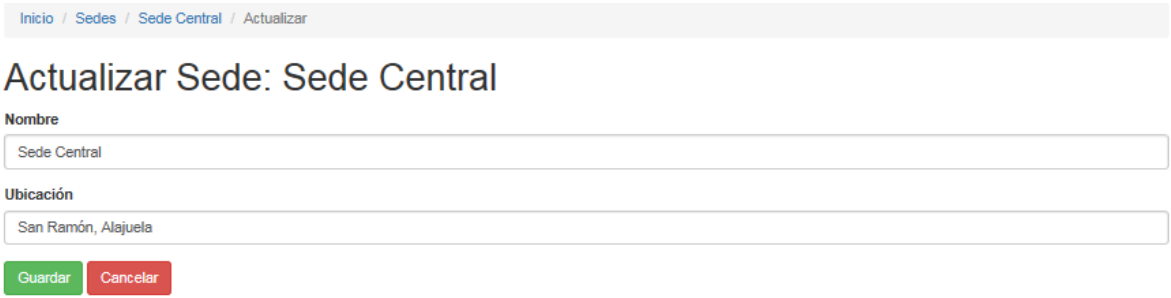
Para eso solo necesita presionar el botón “Agregar sede”, y aparecerá un formulario donde se debe agregar los datos de la nueva sede.



Para este formulario el campo Nombre es requerido, mientras que el espacio Ubicación es deseable, pero se puede crear una Sede sin este.

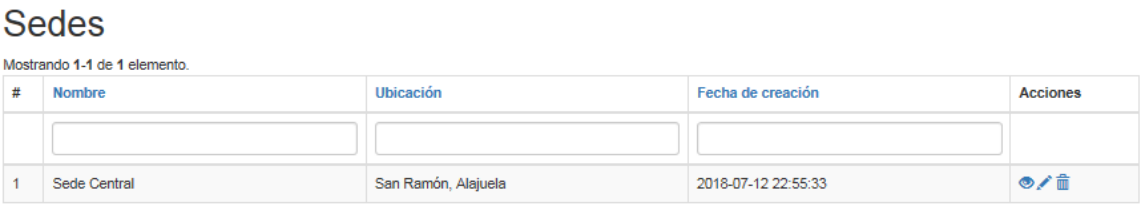
Actualizar sede

Al igual que en el resto de mantenimientos, el usuario tiene la opción de editar una Sede, al presionar el botón “Actualizar” presente en el mantenimiento. Una vez hecho esto aparecerá un formulario con los datos de la sede que se desean modificar y posteriormente salvar



Eliminar Sede

Para eliminar una Sede es necesario que el usuario seleccione un registro dentro de la tabla ubicada en el mantenimiento, y dé clic sobre el botón “Eliminar”, ubicado en la columna acciones (icono de cesto de basura).



Luego de esto aparecerá una ventana con un mensaje de confirmación, con el fin de verificar si el usuario realmente desea llevar a cabo la acción; en caso de que la respuesta sea afirmativa y no tener una evaluación asociada, la sede será eliminada. Si la operación no puede ser llevaba a cabo aparecerá un mensaje informativo con las razones del porqué no se pudo completar la acción.

Anexo 4: Carta autorización Racsa

racsa

San Pedro, Montes de Oca, 21 de diciembre del 2017

Señores
Huberto Pérez Gonzáles
Marlo Soto Elizondo

Estimados señores:

Por este medio se les autoriza para que realicen un estudio acerca de las funcionalidades del componente de firma digital que se utiliza en el Sistema Integrado de Compras Públicas SICOP, el cual se encuentre disponible para que sea descargado por cualquier usuario de la plataforma desde el portal http://www.componentefirmacr.go.cr/ .

Cabe mencionar que la presente autorización es única y exclusivamente para usos de índole académicos, por lo que información obtenida dentro del estudio no podrá ser utilizada con fines comercializales ni se puede extender a terceros.

Se despide muy atentamente.

Licenciado
Oscar Ugarte Medina
Coordinador Proyecto SICOP
Radiográfica Costarricense, S.A.

Archivo

Anexo 5: Carta Patrocinador

MINISTERIO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

DEPARTAMENTO DE RESPUESTA A INCIDENTES INFORMÁTICOS

CSIRT-CR

San José, 06 de Setiembre 2018

Señores
Tribunal Examinador
Universidad Cenfotec

Estimados señores:

Por este medio deseo externar mi agradecimiento a los estudiantes Humberto Pérez González y Marlon Soto Elizondo, de la Maestría en Ciberseguridad de la Universidad Cenfotec, los cuales a través de su tesis titulada **"Creación de una plataforma web segura, para automatizar el modelo de madurez en ciberseguridad ECM2, con el fin de facilitar la tarea de determinar el estado real en materia de ciberseguridad a instituciones sin importar su tamaño o sector",** han superado con creces los resultados esperados para dicho proyecto.

Contar con un sistema web que consolide la información sobre cual es el nivel de madurez en ciberseguridad que poseen las instituciones públicas nos permitirá analizar y evaluar sus capacidades, así como los procesos actuales que deben mejorarse para asegurar la información que se transmite tanto entre entidades como hacia el ciudadano.

El impacto que puede tener este modelo automatizado para el gobierno, es fundamental para apoyar las líneas de acción de la Estrategia Nacional de Ciberseguridad, la cual fue lanzada a finales del año pasado.

Es de suma importancia para el país contar con este tipo de herramientas, que brinden información actualizada de los posibles riesgos y vulnerabilidades existentes en nuestras instituciones del gobierno, de tal forma que podamos generar conciencia sobre lo vital que es la ciberseguridad y a su vez contribuir eficazmente en la prevención de posibles ciberamenazas.

Sin otro particular,

JOHNNY GERARDO PAN SANABRIA (FIRMA)

Digitally signed by JOHNNY GERARDO PAN SANABRIA (FIRMA)
Date: 2018.09.06 08:59:38 -06'00'

Johnny Pan Sanabria
Coordinador CSIRT-CR
Ministerio de Ciencia, Tecnología y Telecomunicaciones