ANÁLISIS DE RIESGOS PARA EL APLICATIVO COPIAS ELECTRÓNICAS

TRABAJO DE GRADO

PARTICIPANTES

Eduar Enrique Navarro Morales
Código: 1622010168

Claudia Marlen Neiva Cortes
Código: 1622010061

Yeison Humberto Latorre Ruiz
Código: 1622010023

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

ANÁLISIS DE RIESGOS PARA EL APLICATIVO COPIAS ELECTRÓNICAS

TRABAJO DE GRADO

PARTICIPANTES

Eduar Enrique Navarro Morales
Código: 1622010168

Claudia Marlen Neiva Cortes
Código: 1622010061

Yeison Humberto Latorre Ruiz
Código: 1622010023

Asesor(es)
Alejandro Castiblanco Caro

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

2017

Nota de aceptación

Firmas de los jurados

Bogotá, Septiembre 17 de 2017.

Introducción

Protección es un ente de control y vigilancia del sector industria, comercio y turismo que ha optado por implementar sistemas de virtualización y desarrollos de aplicaciones in house, en específico la aplicación de Copias Electrónicas, el cual permite gestionar de manera oportuna y eficaz las solicitudes realizadas por los usuarios cuando requieren obtener copias de los documentos que se tramitan en la entidad.

Las entidades del estado deben dar cumplimiento a las directrices de seguridad de la información, eficiencia, cero papel, Gobierno en Línea (GEL), entre otros, generados por los entes de control, quienes invitan a fortalecer al interior de las organizaciones a nivel de TI, replanteando sus procesos y lineamientos con el fin de asegurar y preservar la confidencialidad, integridad y disponibilidad de los activos de información.

En la presente propuesta se toma como referencia el aplicativo Copias Electrónicas, donde a partir de la elaboración de documentos se definen lineamientos de seguridad basados en buenas prácticas de desarrollo de software seguro, gestión de roles y permisos y administración de la infraestructura tecnológica, se hace necesario realizar un análisis de seguridad sobre el aplicativo de copias, en tal sentido lograr estandarizar los procesos para dar cumplimiento a los principios básicos de seguridad de la información.

ÍNDICE

Agradecimientos

Agradecemos a Dios por ofrecernos la oportunidad de crecer personal y profesionalmente, a nuestras parejas e hijos por su apoyo incondicional, porque son nuestra inspiración para luchar día a día por nuestros sueños y por lo que soñamos para ellos, a nuestras familias quienes estuvieron acompañándonos y alentándonos para no desfallecer en el intento.

A todas aquellas personas que nos brindaron apoyo, amigos, docentes y asesores, gracias por sus valiosos aportes, que fueron fundamentales para lograr este importante objetivo, que sin duda es motivo de orgullo, alegría y satisfacción.

1. RESUMEN EJECUTIVO

Protección es un ente de control y vigilancia del sector industria, comercio y turismo que ha optado por implementar sistemas de virtualización y desarrollos de aplicaciones in house, donde en las diferentes etapas de desarrollo se presentan falencias en el Entendimiento del Riesgo, Requerimientos, Diseño, Implementación, Pruebas de seguridad y Publicación Segura, permitiendo que se generen incidentes de seguridad sobre las aplicaciones en específico la aplicación que permite la gestión de copias electrónicas, el cual permite gestionar de manera oportuna y eficaz las solicitudes realizadas por los usuarios cuando requieren obtener copias de los documentos que se tramitan en la entidad.

La aplicación Copias Electrónicas se encuentra instalada y configurada sobre servidores virtuales con sistemas operativos Linux, los cuales no están actualizados, dado que el personal de soporte técnico no tiene planes de actualizaciones periódicas para los servidores; esto ocasiona incidentes de seguridad asociados a la disponibilidad en sus activos de información. De otra parte, la definición de perfiles no son adecuados para la asignación de accesos privilegiados a la información catalogada como reservada, que pueden ocasionar incidentes de seguridad de la información relacionados con confidencialidad e integridad de los datos procesados en el aplicativo.

Teniendo en cuenta que los incidentes de seguridad han aumentado de manera considerable durante los últimos dos años, entre otros los más frecuentes son detección

de fallos en las actualizaciones para los servidores, indisponibilidad de servidores, aplicaciones que incumplen las políticas de seguridad de la entidad, servicios no disponibles, instalación de software no autorizado; la entidad requiere implementar mecanismos que permitan identificar este tipo de eventos que ponen en riesgo sus activos de información, entre ellos evaluar el cumplimiento de las políticas de seguridad definidas en la entidad, en este caso, específicamente en el aplicativo copias electrónicas, lo anterior representa oportunidad de cambio y mejora para los procesos de la entidad.

En este sentido se hace necesario analizar el estado actual de la seguridad de la aplicación Copias Electrónicas, basados en una metodología y un documento para el desarrollo de software seguro que permitan verificar el cumplimiento de los principios básicos de la Seguridad de la Información, con el fin de reducir los riesgos a niveles aceptables y asumibles, ya que actualmente se presenta indisponibilidad del aplicativo Copias de Seguridad de manera constante en un 40% del tiempo en el que debe estar disponible, incrementando así los soportes técnicos generando una carga operativa asociada a los requerimientos realizados por los usuarios, entre otros, transacciones que no finalizan adecuadamente afectando la integridad de los datos, ocasionando inconsistencia en la información registrada.

El análisis de riesgos de la información y la adopción de buenas prácticas para el desarrollo de software seguro, permite tomar decisiones sobre la forma en que se podría mejorar y cumplir a cabalidad los objetivos estratégicos de la entidad, garantizando la confiabilidad, integridad y disponibilidad de la información.

Como objetivo general se propone una metodología que permita identificar, valorar y tratar los riesgos de seguridad de la información, asociados a la confiabilidad, integridad y disponibilidad de la aplicación Copias Electrónicas en la entidad Protección, así mismo generar un documento que contenga los lineamientos para el desarrollo de software seguro al interior de la misma.

Como punto de partida se define la metodología para la identificación, valoración y tratamiento de riesgos de Seguridad de la Información del aplicativo Copias Electrónicas. Se realiza la identificación, valoración y tratamiento de riesgos de Seguridad de la Información del aplicativo Copias Electrónicas.

Para la metodología de gestión de riesgos de seguridad que se adoptará la NTC ISO 31000, Octave Allegro, donde se describe los ítems a tener en cuenta para garantizar el proceso de gestión del riesgo complementándose con la NTC ISO 27001; basados en ello se construye la metodología y se aplica realizando el análisis de riesgos de seguridad del activo de información Aplicativo Copias Electrónicas.

Para la implementación de los controles se tomará como referencia la norma técnica ISO 27001 Anexo A los mismos se aplicarán a los riesgos inherentes identificados, con el fin de que los mismos se mitiguen y posteriormente la valoración de la efectividad del activo.

Para determinar la efectividad de los controles se tomará como guía la metodología propuesta por el Departamento Administrativo de la Función Pública (DAFP), para ello se tendrá en cuenta la tabla de criterios para la valoración de los controles.

Una vez identificados los riesgos a los cuales se encuentra expuesto el aplicativo, se proponen controles a las vulnerabilidades encontradas para mitigarlas, entre ellos la propuesta se genera un documento que contenga los lineamientos existentes para el desarrollo de software seguro, con el fin de aplicarlos al interior de la entidad mejorando la calidad de sus aplicaciones e incentivando la seguridad de la información en las mismas.

El Estándar de Verificación de Seguridad en Aplicaciones (ASVS) del proyecto OWASP se utiliza como un checklist de requerimientos en seguridad para los sistemas de información.

Cada nivel ASVS contiene una lista de requerimientos de seguridad donde cada uno de estos puede también corresponder a funcionalidades específicas de seguridad y capacidades que deben construirse por los desarrolladores de software.

Con la elaboración de los documentos planteados se logró optimizar la evaluación y control de los riesgos a los que está expuesta la aplicación, identificar y priorizar los riesgos que afectan la confidencialidad integridad y disponibilidad asociados al aplicativo; proponer los controles y acciones que se deben implementar para reducir el margen de error por indisponibilidad en las operaciones de la aplicación; contribuir con la política de seguridad de la información, al registrar y tratar los riesgos disminuyendo el número de

incidentes de seguridad, permitir establecer puntos de control durante las pruebas se seguridad entregando servicios estables y eficientes, permite reducir considerablemente la carga de soportes registrados asociados a incidentes de seguridad, ayudando al mejoramiento continuo, plantear una línea base para el análisis de riesgos de las aplicaciones, conforme al planteamiento de la Metodología de Riesgos de Seguridad de la Información como herramienta para la identificación, valoración y tratamiento de riesgos de Seguridad de la Información permitiendo contribuir al logro de los objetivos definiendo los riesgos de seguridad de la información y categorizarlos de forma adecuada de acuerdo a la probabilidad e impacto.

El alcance del proyecto abarca el proceso de Tecnologías de la Información de Protección, generando una metodología que permita realizar la identificación, valoración y tratamiento de riesgos, hasta proponer los controles a los riesgos identificados, como parte del Sistema de Gestión de Seguridad de la Información en su fase planear al aplicativo Copias Electrónicas de la entidad Protección, y generar un documento que contenga los lineamientos existentes para el desarrollo de software seguro al interior de la entidad.

La implementación de los mecanismos que mitiguen la ocurrencia de los riesgos no se contempla dentro del presente alcance.

2. JUSTIFICACIÓN

Teniendo en cuenta que los incidentes de seguridad han aumentado de manera considerable durante los últimos dos años, entre otros los más frecuentes son detección de fallos en las actualizaciones para los servidores, indisponibilidad de servidores, aplicaciones que incumplen las políticas de seguridad de la entidad, servicios no disponibles, instalación de software no autorizado; por tal razón la entidad requiere implementar mecanismos que permitan identificar este tipo de eventos que ponen en riesgo sus activos de información, entre ellos evaluar el cumplimiento de las políticas de seguridad definidas en la entidad, en este caso, específicamente en el aplicativo copias electrónicas, lo anterior representa oportunidad de cambio y mejora para los procesos de la entidad.

En este sentido se hace necesario analizar el estado actual de la seguridad de la aplicación Copias Electrónicas, basados en una metodología y un documento para el desarrollo de software seguro que permitan verificar el cumplimiento de los principios básicos de la Seguridad de la Información, con el fin de reducir los riesgos a niveles aceptables y asumibles, ya que actualmente se presenta indisponibilidad del aplicativo de manera constante en un 40% del tiempo en el que debe estar disponible, incrementando así los soportes técnicos generando una carga operativa asociada a los requerimientos realizados por los usuarios, entre otros, transacciones que no finalizan adecuadamente afectando la integridad de los datos, ocasionando inconsistencia en la información registrada.

De otra parte, no se cuenta con herramientas de monitoreo que permiten evidenciar el tipo y vulnerabilidades a los que se encuentra expuesta la aplicación copias electrónicas, por consiguiente se hace necesario realizar el análisis de riesgo de la aplicación con el fin de obtener indicadores que permitan tener trazabilidad de las vulnerabilidades de la aplicación y en una segunda fase del proyecto implementar mecanismos que las mitiguen.

Acogiendo los parámetros planteados en la Estrategia de Gobierno en Línea (GEL) liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones, donde se recopilan instrumentos técnicos, normativos y de política pública que promueven la construcción de un Estado más eficiente, transparente y participativo mediante el aprovechamiento de la tecnología, para ofrecer a la ciudadanía garantía sobre la información que se procesa en la entidad.

El análisis de riesgos de la información y la adopción de buenas prácticas para el desarrollo de software seguro, permite tomar decisiones sobre la forma en que se podría mejorar y cumplir a cabalidad los objetivos estratégicos de la entidad, garantizando la confiabilidad, integridad y disponibilidad de la información.

3. MARCO TEÓRICO Y REFERENTES

- **Amenaza:** Evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización.

- **Impacto:** Daño potencial sobre un sistema cuando una amenaza se presenta.

- **Norma ISO 270001: 2013 Sistemas Gestión de Seguridad de la Información:** Entrega los requisitos para el establecimiento, la implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información al interior de las organizaciones.

- **Norma ISO 31000: 2011 Gestión del Riesgo:** Las organizaciones de todo tipo y tamaño enfrentan factores e influencias, internas y externas, que crean incertidumbre sobre si ellas lograrán o no sus objetivos. El efecto que esta incertidumbre tiene en los objetivos de una organización es el “riesgo”.

  Todas las actividades de una organización implican riesgo. Las organizaciones gestionan el riesgo mediante su identificación y análisis; luego evaluando si el riesgo se debería modificar por medio del tratamiento del riesgo con el fin de satisfacer los criterios. A través de este proceso, las organizaciones se comunican y consultan con las partes involucradas, monitorean y revisan el riesgo y los controles que lo están modificando con el fin de garantizar que no se requiere tratamiento adicional para el mismo. Esta norma describe este proceso sistemático y lógico en detalle.

- **Plan de Continuidad del Negocio:** Estrategia planificada constituida por: un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio afectados por una paralización total o parcial de la capacidad operativa de la empresa.

- **Riesgo:** Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.

- **Octave Allegro:** Técnica de planificación y consultoría estratégica en seguridad basada en el riesgo y prácticas de seguridad, permitiendo a las organizaciones tomar decisiones de protección de la información basados en los tres pilares confidencialidad, integridad y disponibilidad de la misma.

- **Sistema de Información.** Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

- **Top 10 Owasp:** Existen cientos de problemas que pueden afectar la seguridad en general de una aplicación web, este top 10 da a conocer una lista de las vulnerabilidades más comunes de las aplicaciones web y su descripción. En su sitio oficial también publica recomendaciones para dar manejo a dichas vulnerabilidades, y así generar desarrollos seguros en el mercado.

- **Vulnerabilidad:** Cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas para la organización.

4. METODOLOGÍA

A continuación la descripción de los métodos adoptados con el fin de desarrollar la solución propuesta al problema relacionado con la aplicación Copias Electrónicas, identificado al interior de la entidad Protección, de acuerdo a lo planteado en alcance de este proyecto.

Esta metodología tendrá como referencia las normas técnicas NTC ISO 31000, Octave Allegro, donde se describen los ítems a tener en cuenta para garantizar el proceso de gestión del riesgo, así mismo la NTC ISO 27001, estándar para la seguridad de la información.

El proyecto se ha desarrollado bajo los parámetros de una investigación tipo factible, toda vez que de acuerdo a su definición se ajusta perfectamente a lo que se pretende, que es generar una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales. Dado lo anterior, el proyecto corresponde al análisis de riesgos del aplicativo Copias Electrónicas, lo cual originará propuestas de mejora; como la documentación de una metodología que describe el paso a paso para realizar el análisis de riesgo al mencionado aplicativo, una vez identificados los riesgos a los cuales se encuentra expuesto el aplicativo, se proponen controles a las vulnerabilidades encontradas para mitigarlas, entre ellos la propuesta de un documento que contiene los lineamientos de Buenas Prácticas para el Desarrollo de Software Seguro, basado en criterios a tener en cuenta para el cumplimiento de aplicaciones seguras.

5. RESULTADOS Y DISCUSIÓN

Con la elaboración de los documentos planteados, es pertinente señalar, que la metodología y el documento de buenas prácticas de desarrollo seguro, al ser aplicados al interior de la entidad, mejoran la calidad de sus procesos e incentiva la cultura de seguridad de la información, los documentos deben irse actualizando de acuerdo a las necesidades y requerimientos de la entidad, usuarios funcionales, la normativa vigente y contando con la definición de nuevos lineamientos que permitan abarcar otros aplicativos, teniendo en cuenta una línea base para el análisis de riesgos de las aplicaciones, conforme al planteamiento de la Metodología de Riesgos de Seguridad de la Información para el aplicativo Copias Electrónicas, que sirve como herramienta para la identificación, valoración y tratamiento de riesgos de Seguridad de la Información en relación al aplicativo Copias Electrónicas, permitiendo contribuir al logro de los objetivos estratégicos, definiendo correctamente los riesgos de seguridad de la información y categorizarlos riesgos de forma adecuada de acuerdo a la probabilidad e impacto.

Logrando así cumplir con la propuesta de una metodología que permita identificar, valorar y tratar los riesgos de seguridad de la información, asociados a la confiabilidad, integridad y disponibilidad de la aplicación Copias Electrónicas en la entidad Protección,

así mismo generar un documento que contenga los lineamientos para el desarrollo de software seguro al interior de la misma.

6. CONCLUSIONES

Con base al trabajo realizado se logró establecer una metodología que permite realizar un análisis de los riesgos a los cuales se encuentra expuesta la aplicación de copias Electrónicas.

A partir de la definición de la metodología se establece una línea base que sirve para realizar el análisis de riesgos de las diferentes aplicaciones de la Entidad, estableciendo unos criterios mínimos de seguridad que permitan fortalecer el proceso de seguridad de la información al interior de la Entidad.

Teniendo en cuenta el análisis realizado se proponen controles que permitan mitigar la ocurrencia de riesgos complementando estos controles con una serie de recomendaciones a seguir con el fin de asegurar la aplicación en base al documento buenas prácticas de desarrollo seguro.

Como parte del aseguramiento de acuerdo al análisis realizado se definen lineamientos de seguridad como criterios mínimos que deben dar cabal cumplimiento el equipo de desarrolladores, permitiendo garantizar un nivel de cumplimiento mínimo en relación a las 10 vulnerabilidades definidas en el proyecto Owasp top ten.

7. BIBLIOGRAFÍA

OWASP, Los diez riesgos más críticos de Aplicaciones Web [en línea] 2013 Disponible en https://www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf

OWASP, Los diez riesgos más importantes en Aplicaciones Web [en línea] 2010 Disponible en https://www.owasp.org/images/2/2d/OWASP_Top_10_-_2010_FINAL_(spanish).pdf

RAMOS P, La realidad de la seguridad empresarial en Latinoamérica: ¿qué debemos hacer? [en línea] 2016 Disponible en http://www.welivesecurity.com/la-es/2016/04/29/seguridadempresarial-latinoamerica-que-hacer/

ENYOYSAFERTECHNOLOGY, Eset Security Report Latinoamérica 2014 [en línea] 2014 Disponible en http://www.welivesecurity.com/wp-content/uploads/2014/06/informe_esr14.pdf

RAMOS P, 5 Preguntas para el equipo de Seguridad de tu empresa [en línea] 2014 Disponible en http://www.welivesecurity.com/la-es/2014/08/27/5-preguntas-equipo-seguridad-empresa/

MINTIC, Seguridad y Privacidad de la Información, Guía de indicadores de gestión para la seguridad de la información [en línea] 2015 Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

WHITE HAT SECURITY, Website Security StatisticsReport [en línea] 2013 Disponible en https://www.whitehatsec.com/wp-content/uploads/2013/05/WPstatsReport_052013.pdf

Almanza A, ACIS, Tendencias 2016 Encuesta nacional de seguridad informática [en línea] 2016 Disponible en http://acis.org.co/revista139/content/tendencias-2016-encuesta-nacional-de-seguridad-inform%C3%A1tica

Certisi, Actualización y seguridad para el kernel [en línea] disponible en https://www.certsi.es/search/site/linux?page=1

ISO/IEC 27001:2013, Tecnología de la información. Técnica de Seguridad. Código de práctica para Controles de seguridad de la Información.

ISO/IEC 31000:2011, Gestión del Riesgo.

Francisco Monseratt. Incidentes de seguridad en equipos Linux [en línea] disponible en http://www.othlo.com/htecnologia/documentacion/hispalinux04/05seglinux.pdf

Mintic. Controles de Seguridad y Privacidad de la Información [en línea] disponible enhttp://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

SIGEPRE; LINEAMIENTO DE DESARROLLO DE PROYECTOS DE SOFTWARE Agosto 2016; http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/L-TI-14-Desarrollo-Software.pdf

GOBIERNO EN LÍNEA; ESTRATEGIA GOBIERNO EN LÍNEA; http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7652.html

http://www.redalyc.org/pdf/410/41030203.pdf

BSIMM, Url: https://go.bsimm.com/hubfs/BSIMM/BSIMM7.pdf

OWASP, Application Security Verification Standard 3.0.1 July 2016, Url: https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf

OWASP, Estándar de Verificación de Seguridad en Aplicaciones 3.0.1 Versión en español: Abril de 2017 Url: https://www.owasp.org/images/a/aa/Est%C3%A1ndar_de_Verificaci%C3%B3n_de_Seguridad_en_Aplicaciones_3.0.1.pdf

Software Assurance Maturity Model, Una guía para integrar seguridad en el desarrollo de software Url: http://www.opensamm.org/downloads/SAMM-1.0-es_MX.pdf

Building Security In Maturity Model (BSIMM), Url: http://www.fundacionsadosky.org.ar/wp-content/uploads/2014/07/BSIMM-V-esp.pdf

Aguilera V, Controles Técnicos de Seguridad para la Protección de Aplicaciones Web, Url: http://www.vicenteaguileradiaz.com/pdf/SIC94_Seguridad_Aplicaciones_OWASP.pdf

GOBIERNO DE CANARIAS; Normativa sobre los requisitos de Seguridad en Aplicaciones Web; Url: https://www.gobiernodecanarias.net/cmsgobcan/export/sites/cibercentro/pdf/documentos_pdf/normativas_pdf/DGTNT-012981-TSI-NORM-SEG_Normativa_sobre_los_requisitos_de_Seguridad_en_Aplicaciones_Web.pdf

R Moises, Experiencias en la Industria del Software: Certificación del Producto con ISO/IEC 25000BSIMM, Url: http://eventos.spc.org.pe/cibse2015/pdfs/01_IT15.pdf

OWASP, Anexo para Contrato de Software Seguro de OWASP Url: https://www.owasp.org/index.php/Anexo_para_Contrato_de_Software_Seguro_de_OWASP

OWASP, Download zaproxy Url: https://github.com/zaproxy/zaproxy/wiki/Downloads

Proyecto Top Ten de OWASP Url: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

https://www.gobiernodecanarias.net/cmsgobcan/export/sites/cibercentro/pdf/documentos_pdf/normativas_pdf/DGTNT-012981-TSI-NORM-SEG_Normativa_sobre_los_requisitos_de_Seguridad_en_Aplicaciones_Web.pdf

Javier Ginebreda Galofre (2013), Segregación de Funciones, Recuperado de: https://upcommons.upc.edu/bitstream/handle/2099.1/20387/PFC%20Memoria.pdf

jpgarcia.cl, Autorización basada en roles RBAC, la definición inicia, Recuperado de: https://jpgarcia.cl/2007/04/05/autorizacion-basada-en-roles-rbac-la-definicion-inicial/

IBM, Modelo de Acceso, Recuperado de: https://www.ibm.com/support/knowledgecenter/es/SSTFWV_5.1.0/com.ibm.itim.doc/cpt/cpt_ic_plan_role_issues_models_acc.html

8. ANEXOS

8.1 METODOLOGÍA RIESGOS DE SEGURIDAD DE LA INFORMACIÓN APLICATIVO COPIAS ELECTRÓNICAS.

La presente metodología permite documentar las actividades propias del Análisis de Riesgos de la Información para el aplicativo Copias Electrónicas, acogiendo como primera medida los parámetros planteados en la Estrategia de Gobierno en Línea (GEL) liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones, el cual recopila instrumentos técnicos, normativos y de política pública que promueven la construcción de un Estado más eficiente, transparente y participativo mediante el aprovechamiento de la tecnología.

Mediante la implementación de esta metodología se pretende establecer lineamientos que aporten a la protección del activo de información, Aplicativo Copias Electrónicas, mitigando los riesgos informáticos y salvaguardándolos, ya que éstos son parte primordial para el cumplimiento de los objetivos estratégicos de la entidad.

ALCANCE

El alcance de la metodología propuesta en este documento comprende la identificación y análisis de los riesgos más relevantes para el aplicativo Copias Electrónicas, se categorizará y determinará la probabilidad e impacto sobre el activo de información, con el fin de proponer controles que permitan mitigar el impacto sobre él.

En cuanto a la metodología Octave allegro de gestión de riesgos de seguridad, la NTC ISO 31000, donde se describe los ítems a tener en cuenta para garantizar el proceso de gestión del riesgo complementándose con la NTC ISO 27001.

OBJETIVOS

OBJETIVO GENERAL

Proponer una metodología que permita definir correctamente los riesgos de seguridad de la información y categorizarlos de forma adecuada de acuerdo a la probabilidad e impacto.

OBJETIVOS ESPECÍFICOS

- Identificar los riesgos a los que se encuentra expuesta la información del aplicativo Copias Electrónicas.

- Analizar los riesgos encontrados para el aplicativo Copias Electrónicas.

- Proponer controles que permitan mitigar los riesgos calificados como catastróficos del aplicativo Copias Electrónicas.

ANÁLISIS DE RIESGOS DE LA INFORMACIÓN

El adecuado manejo de los riesgos favorece el desarrollo y crecimiento de la entidad, con el fin de asegurar dicho manejo, es importante que se establezca el entorno y ambiente organizacional de la entidad, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos, esto en desarrollo de los siguientes elementos:

- Comunicación y consulta periódicamente.
- Establecer el contexto: mapa de procesos.
- Identificación del activo de información.
- Valoración del activo de información.
- Identificación de los riesgos.
- Valoración de riesgos.
- Análisis de los riesgos.
- Evaluación de los riesgos.
- Tratamiento de los riesgos: para eliminar, mitigar o transferir el riesgo.

IDENTIFICACIÓN DE LA INFORMACIÓN

Para la identificación y clasificación de la información del aplicativo Copias Electrónicas se tendrán en cuenta los siguientes aspectos:

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

El esquema de identificación de la información estará asociado al sistema de información, sus respectivos propietarios y su ubicación.

El inventario será actualizado por cada unidad organizativa y revisado con periodicidad semestral.

En este inventario se debe identificar el nombre del activo, descripción (características del activo de información), responsable (nombre de la dependencia a la cual pertenece el activo de información), custodio (es quien resguarda el activo de información), contenedores de información (son todos los lugares por donde pasa la información).

El propietario de cada activo es el responsable de clasificar la información de acuerdo a la importancia de esta y almacenar y manejar su información de acuerdo con el nivel de clasificación.

Para el nivel de clasificación de los activos de información se tendrán en cuenta los siguientes criterios:

Criterios de Valoración Activos					
Criterios			Impacto		
Confidencialidad	Integridad	Disponibilidad	Financiero	Legal	Imagen

Tabla 1 Criterios de Valoración Activos

Una vez clasificados los activos de información, se procede a realizar la valoración de activos.

VALORACIÓN DEL ACTIVO

La criticidad del activo se determinará a partir de la sumatoria de los impactos organizacionales en relación a los criterios de confidencialidad, integridad y disponibilidad del activo.

NIVELES DE IMPACTO EN EL ACTIVO

Una vez identificados los activos de información se procederá a valorar su grado de importancia y criticidad para la entidad, para lo cual, se debe valorar la afectación que le puede generar a la entidad en cuanto al impacto financiero, legal y de imagen, en caso dado que al materializarse una amenaza que afecte su disponibilidad, integridad o confidencialidad. Para esto utilizaremos los siguientes criterios:

Tabla Valoración Activos de información				
Impacto	**Descripción**	**Escala Cuantitativa**	**Escala de Valoraci**	**Concepto**
Financiero	Reducción en la asignación del presupuesto de la siguiente vigencia	**1**	**Muy Bajo**	Menor o igual al 8% de disminución del presupuesto anual asignado a la entidad
		2	**Bajo**	Mayor al 9% y menor o igual 14% de disminución el presupuesto anual asignado a la entidad
		3	**Medio**	Mayor al 15% menor o igual 24% de disminución el presupuesto anual asignado a la entidad
		4	**Alto**	Mayor al 25% menor o igual 34% de disminución el presupuesto anual asignado a la entidad
		5	**Muy Alto**	Mayor al 35% menor o igual 50% de disminución el presupuesto anual asignado a la entidad
Legal	Incumplimiento de la normatividad	**1**	**Muy Bajo**	No tiene repercusión frente a normatividad
		2	**Bajo**	Investigación Disciplinaria
		3	**Medio**	Demandas y/o Multas
		4	**Alto**	Investigación Fiscal
		5	**Muy Alto**	Intervención - Sanción
Imagen	Afectación de la imagen ante el sector y la ciudadanía	**1**	**Muy Bajo**	Los objetivos no se ven afectados al Interior de la entidad
		2	**Bajo**	Los objetivos se ven afectados al interior de la entidad
		3	**Medio**	Los objetivos de la entidad se ven afectados a nivel sectorial
		4	**Alto**	Los objetivos de la entidad se ven afectados a nivel regional
		5	**Muy Alto**	Los objetivos de la entidad se ven afectados en el Orden Nacional

Tabla 2 Valoración Activos de Información

Criterio	Impacto	Descripción
Confidencialidad	Financiero	¿Si la información del activo es divulgada qué impacto financiero se puede generar?
	Legal	¿Si la información del activo es divulgada qué impactos legales se pueden generar?
	Imagen	¿Si la información del activo es divulgada como puede afectar la imagen de la entidad?
Integridad	Financiero	¿Si el activo de información es alterado qué impacto financiero se puede generar?
	Legal	¿Si el activo de información es alterado qué impactos legales se pueden generar?
	Imagen	¿Si el activo de información es alterado como puede afectar la imagen de la entidad?
Disponibilidad	Financiero	¿Si el activo de información no se encuentra disponible qué impacto financiero se puede generar?
	Legal	¿Si el activo de información no se encuentra disponible qué impactos legales se pueden generar?
	Imagen	¿Si el activo de información no se encuentra disponible como puede afectar la imagen de la entidad?

Tabla 3 Criterio Vs Impacto

Para obtener el nivel de criticidad del activo se deben tener en cuenta los siguientes de rangos:

Tabla de Criticidad		
RANGO	NIVEL	DESCRIPCIÓN
9-13	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o'efectos mínimos sobre la entidad.
14-19	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
20-28	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
29-38	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
39-45	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Tabla 4 Criticidad Activo de Información

IDENTIFICACIÓN DE LOS RIESGOS

La recolección de la información se realizará mediante la técnica lluvia de ideas en conjunto con el líder del proceso quien conoce las falencias de éste. Una vez terminado el listado de dichos riesgos, se incorporarán en la matriz de riesgos de acuerdo al contexto establecido en las actividades del proceso.

En el listado de riesgos detectados se debe indicar para cada uno:

- Un código identificativo, que permite mantener la trazabilidad de los riesgos dentro del proceso.
- Nombre del activo de información.
- Amenaza.
- Vulnerabilidad.
- Nombre del riesgo.
- Riesgo (breve descripción del riesgo).
- Criterio.

IDENTIFICACIÓN Y ANÁLISIS DE LOS RIESGOS					
Id Riesgo	Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Criterio

Tabla 5 Identificación de los Riesgos

ANÁLISIS DE LOS RIESGOS

Probabilidad: Para obtener el nivel de la probabilidad que una vulnerabilidad potencial pueda materializarse dentro del activo de información se tendrán en cuenta los siguientes criterios:

TABLA DE PROBABILIDAD		
Escala Cuantitativa	Escala de Valoración	DESCRIPCIÓN
1	Raro	La amenaza carece de motivación. Los controles son suficientes para evitar que la vulnerabilidad suceda
2	Improbable	La de amenaza es motivada pero no es capaz. Los controles están listos para prevenir o para impedir significativamente que la vulnerabilidad suceda
3	Posible	La amenaza es motivada y capaz. Los controles pueden impedir el éxito de que la vulnerabilidad suceda
4	Probable	La amenaza es medianamente motivada y suficientemente capaz. Los controles para prevenir que la vulnerabilidad suceda son ineficientes
5	Casi seguro	La amenaza es altamente motivada y suficientemente capaz. No existe los controles necesarios para prevenir que la vulnerabilidad suceda

Tabla 6 Probabilidad del Riesgo

Impacto: El nivel de impacto corresponde a (cantidad que está en juego o las consecuencias, ya sean positivas o negativas) que tendría cada riesgo si ocurriera; para ello se utilizará una escala estándar con los siguientes niveles:

TABLA DE IMPACTO		
Escala Cuantitativa	Escala de Valoración	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Tabla 7 Impacto del Riesgo

EVALUACIÓN DE LOS RIESGOS

Para evaluar los riesgos se determina su gravedad, clasificándolos en cuatro tipos: baja, moderada, alta y extrema, tal como se presenta a continuación.

Matriz de Calificación	
Escala Cuantitativa	**Escala de Valoración**
B	Zona de riesgo baja
M	Zona de riesgo media
A	Zona de riesgo alta
E	Zona de riesgo extrema

Tabla 8 Matriz de Calificación

Los riesgos se clasificaran según los datos de la tabla anterior, los cuales se obtendrán a partir de los resultados de cruzar las variables de probabilidad e impacto, en una matriz que define la zona de gravedad del riesgo. La matriz que determina los niveles de riesgo y su prioridad que se presenta a continuación:

MAPA DE RIESGO					
PROBABILIDAD	**IMPACTO**				
	Insignificante	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

Tabla 9 Evaluación del Riesgo Cruce de Variables

RIESGO ACTUAL

Para facilitar la calificación y evaluación de los riesgos se realiza la clasificación de los riesgos en una matriz denominada Mapa de riesgo actual, como por ejemplo:

MAPA DE RIESGO ACTUAL					
PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Raro (1)					
Improbable			R8, R9, R10,	R4	
Posible (3)			R1, R2, R3,		
Probable (4)					
Casi Seguro					

Tabla 10 Matriz de Riesgo Inherente

TRATAMIENTO DE LOS RIESGOS

Para el tratamiento de los riesgos se tendrán en cuenta algunas de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto.

Matriz deEvaluación y Respuesta a los Riesgos		
Escala Cuantitativa	DESCRIPCIÓN	
B	Asumir el riesgo	Se asume el riesgo inherente , se debe valorar periódicamente si el riesgo se mantiene en este
M	Reducir el riesgo a largo plazo	Los riesgos podrían tratarse a corto o mediano plazo
A	Reducir el riesgo	Deben adoptarse de forma urgente las medidas necesarias para reducir el riesgo.
E	Reducir, compartir o transferir el riesgo	Se debe reducir el impacto de forma inmediata, tomar las medidas necesarias para evitar la materializacion del riesgo, de ser necesario compartir y transferir el riesgo con un tercero

Tabla 11 Matriz Evaluación y Respuesta a los Riesgos

Evitar el riesgo: Son las acciones encaminadas a prevenir la materialización del riesgo. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.

Reducir el riesgo: Son las acciones encaminadas a disminuir la probabilidad (medidas de prevención) o el impacto (medidas de protección). Si el riesgo no puede ser evitado porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo

nivel posible. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles, se consigue mediante la optimización de los procedimientos y la implementación de controles.

Compartir el riesgo: Son las acciones encaminadas a buscar respaldo y compartir con otro parte del riesgo, reduce su efecto a través del traspaso de las pérdidas a otros procesos o dependencias, como en el caso de los contratos de seguros. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.

Transferir el riesgo: Son las acciones encaminadas a eliminar el riesgo mediante el cambio de responsabilidad o carga por las pérdidas a otra Entidad, mediante legislación, contrato, convenios u otros medios.
Asumir un riesgo: Luego de que el riesgo ha sido reducido transferido puede quedar un riesgo residual que se mantiene, en este caso el responsable del proceso simplemente acepta la pérdida residual probable.

Planes de Contingencia: Parte del plan de manejo de riesgos que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la entidad.

Una vez definida la opción de tratamiento del riesgo (evitar, reducir, compartir, transferir, asumir) se deben establecer nuevos controles que permitan eliminar las causas del riesgo, para ello utilizar la siguiente Tabla:

Evaluación del Riesgo		ID Control	Controles	Tipo del control (Probabilidad/ Impacto)
Zona de Riesgo	Evaluación y Respuesta a los Riesgos			

Tabla 12 Tratamiento de los Riesgos

DISEÑO DE CONTROLES

Para el diseño de los controles se debe tener en cuenta que los mismos son necesarios para salvaguardar y proteger la información de la entidad, buscando mantener la confidencialidad, integridad y disponibilidad. Los controles que se implementen deben mitigar aspectos como, impacto o probabilidad a los riesgos identificados.

TIPOS DE CONTROLES

Para la implementación de los controles se definen tres tipos de controles.

|Categoría	Características
Correctivo	Reducir el impacto de una amenaza Solucionar los problemas descubiertos por los controles defectivos Identificar las causas de un problema o incidente Modificar el (los) sistema(s) de procesamiento para reducir las futuras ocurrencias del problema
Preventivo	Evitar problemas antes de que aparezcan. Monitorear tanto las operaciones como las transacciones de entrada. Tratar de predecir problemas potenciales antes de que ocurran y hacer ajustes. Prevenir la ocurrencia de un error, omisión o acto delictivo.
Defectivo	Controles que detectan un error, alerta o acto delictivo que haya ocurrido y reporta la ocurrencia del ataque

Tabla 13 Categorías Controles

Para la implementación de los controles se tendrán en cuenta los siguientes aspectos:

ID Control	Controles	Tipo del control (Probabilidad/ Impacto)	Categoría

IMPLEMENTACIÓN DE CONTROLES

Para la implementación de los controles se tomará como referencia la norma técnica ISO 27001 Anexo A los mismos se aplicarán a los riesgos inherentes identificados, con el fin de que los mismos se mitiguen y posteriormente la valoración de la efectividad del activo.

VALORACIÓN DE CONTROLES

Para calcular el riesgo residual se debe valorar la efectividad de los controles aplicados a los riesgos identificados.

Para determinar a la efectividad de los controles se tomará como guía la metodología propuesta por el Departamento Administrativo de la Función Pública (DAFP), para ello nos apoyaremos en la tabla de criterios para la valoración de los controles.

Criterios de Evaluacion Efectividad del Control		
Aspectos a Evaluar	**Opciones de Respuesta**	**Valor**
Categoría	Control Preventivo	20
	Control Detectivo	15
	Control Correctivo	5
Existe Herramienta para Ejercer el Control	SI/NO	15/0
Están Definidos los Responsables de ejecución y seguimiento	SI/NO	15/0
Frecuencia de Ejecución y Seguimiento Adecuada	SI/NO	20/0
Tiempo de Ejecución Efectivo	SI/NO	20/0
Está Documentado los Pasos para el manejo del control	SI/NO	10/0

Tabla 14 Criterios de Evaluación Efectividad del Control

Después de realizar la valoración para cada uno de los controles y de acuerdo a los valores para cada criterio, la sumatoria del mismo nos dará un rango, que permitirá definir si el control mitigó la probabilidad o el impacto para cada uno de los riesgos.

Tratamiento de riesgo									
ID Control	Controles	Tipo del control (Probabilidad/ Impacto)	Evaluación del Control						
			Categoría	Existe Herramienta para Ejercer el Control	Están Definidos los Responsables de ejecución y seguimiento	Frecuencia de Ejecución y Seguimiento Adecuada	Tiempo de Ejecución Efectivo	Está Documentado los Pasos para el manejo del control	Efectividad del Control

Tabla 15 Tratamiento del Riesgo

RIESGO RESIDUAL

Con base en el resultado de la valoración de los controles y de acuerdo al valor de la efectividad, se determina el desplazamiento en el mapa de calor de los riesgos. De igual forma como en la valoración de los controles, se tomará como referencia la metodología el Departamento Administrativo de la Función Pública.

A continuación se establecen los criterios, para identificar los valores de disminución en cuanto a probabilidad o impacto.

Efectividad del Control	Dependiendo si el control afecta Probabilidad o Impacto	
	Niveles a disminuir en la probabilidad	Niveles a disminuir en el impacto
Entre 0 y 50 puntos	0	0
Entre 51 y 75 puntos	1	1
Entre 76 y 100 puntos	2	2

Tabla 16 Efectividad del Control

Posterior a la valoración y a la disminución de los criterios de valoración de riesgo en cuanto a impacto o probabilidad obtendremos una nueva valoración para cada uno de los riesgos y se clasifican en una nueva matriz denominada mapa de riesgo deseado.

MAPA DE RIESGO DESEADO					
PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Raro (1)			R2, R4, R5, R6,		
Improbable (2)			R3, R11		
Posible (3)	R7	R1			
Probable (4)					
Casi Seguro (5)					

Tabla 17 Mapa de riesgo deseado

8.2 ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL APLICATIVO COPIAS ELECTRÓNICAS, DE ACUERDO A LA METODOLOGÍA DEFINIDA.

Mediante este análisis se podrán identificar las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir en el aplicativo Copias Electrónicas y en el servicio que presta la entidad Protección a la ciudadanía.

8.3 DOCUMENTO BUENAS PRÁCTICAS DESARROLLO DE SOFTWARE SEGURO.

Este documento permite consolidar recomendaciones y mejores prácticas utilizadas en el ciclo de desarrollo de software seguro, como punto de partida para evaluar la seguridad de las aplicaciones y sus artefactos, utilizando criterios de verificación en diferentes etapas del desarrollo y en distintos niveles, aportando al cumplimiento de una estrategia organizacional en seguridad que contribuya al mejoramiento continuo del desarrollo de las aplicaciones.

INTRODUCCION

Las aplicaciones web son accesibles desde diferentes ubicaciones convirtiéndose para usuarios malintencionados en objetivos de ataque, esto a causa de malas configuraciones y defectos en su codificación.

Con el presente documento se dan recomendaciones sobre las actividades a seguir en cada una de las fases del ciclo de vida del desarrollo seguro, que sirven para construir aplicaciones más confiables para los usuarios.

Como punto de partida se apoya en los requerimientos de seguridad de ASVS (Aplication Security Verification Standard) brindando una lista de verificación en cumplimiento a tres niveles de seguridad.

GLOSARIO

ASVS: Estándar de Verificación Seguridad en Aplicaciones
OWASP: Proyecto Abierto de Seguridad en Aplicaciones Web
SAMM: Modelo de madurez para el aseguramiento del software

ALCANCE

El alcance de este documento es plantear algunas prácticas de seguridad y puntos de control que se recomiendan dentro de las fases del ciclo de vida del desarrollo de software, brindando herramientas que apoyen y fortalezcan la seguridad de los sistemas de información.

OBJETIVO

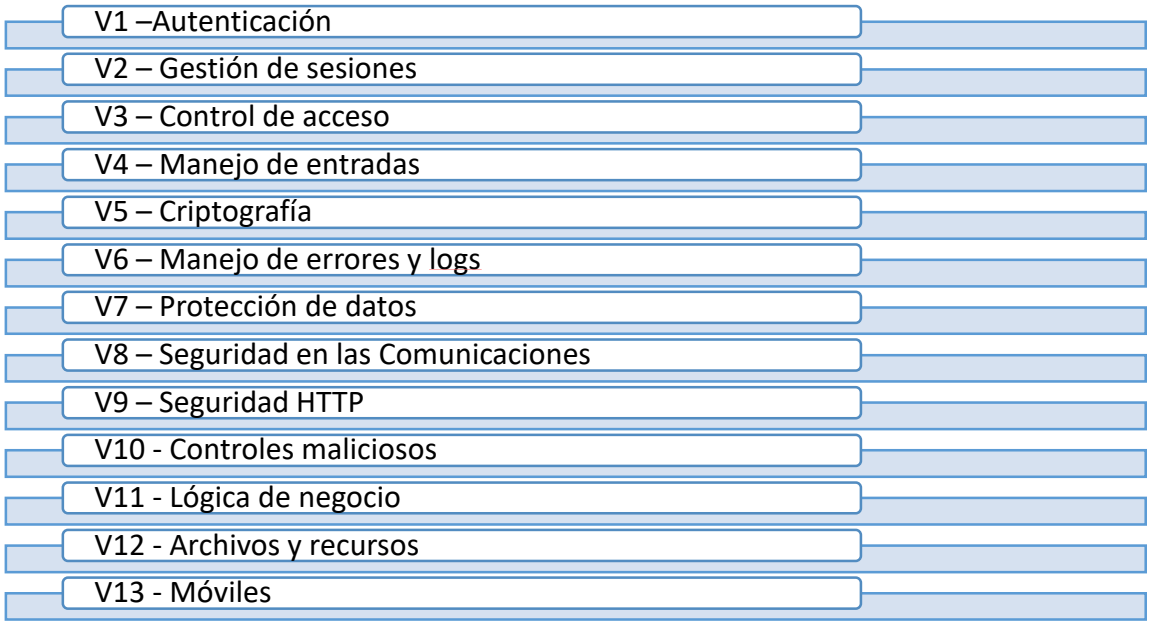
Proponer prácticas de seguridad a incluir en un ciclo de vida de desarrollo seguro en las fases de requerimientos, diseño, implementación pruebas y publicación segura.

OWASP ASVS (APPLICATION SECURITY VERIFICATION STANDARD)

El estándar de verificación de seguridad en aplicaciones es una lista de verificación de requerimientos de seguridad o pruebas que se utiliza para diseñar, desarrollar, probar y definir que tan segura es una aplicación.

El estándar define 3 niveles de verificación de seguridad, incrementando la profundidad en cada uno de los niveles, Nivel 1 mínimo recomendable para cualquier aplicación accesible desde internet, Nivel 2 recomendado para aplicaciones que gestionan información interna de valor medio, Nivel 3 recomendado para aplicaciones que gestionan información de valor alto.

Las categorías en las que se clasifican los requerimientos son:



SEGURIDAD EN LAS FASES DEL CICLO DE DESARROLLO DE SOFTWARE SEGURO

Fase Requerimientos: Las prácticas relacionadas en esta fase corresponden a casos de abuso, requerimientos de seguridad, análisis arquitectónico, modelo arquitectónico, modelo de amenazas y modelo de ataques.

Fase Diseño: Las prácticas de seguridad relacionadas en esta fase corresponden al análisis de riesgo arquitectónico, modelo de amenazas, patrones de diseño, pruebas de seguridad basadas en riesgo y modelos de ataques.

Fase Implementación: Las prácticas de seguridad relacionadas en esta fase corresponden al modelado de ataques y revisión de código.

Fase Pruebas: Las prácticas de seguridad relacionadas en esta fase corresponden a modelado de ataques.

Fase Publicación segura: Las prácticas de seguridad relacionadas en esta fase corresponden al análisis de riesgo arquitectónico, modelo de amenazas, modelado de ataques, test de penetración, configuraciones seguras y operaciones de seguridad.

ACTIVIDADES EN EL CICLO DE DESARROLLO

Fase de requerimientos:

La actividad de casos de abuso permite comprender mejor las áreas de riesgo del sistema, estos casos son la inversa de los casos de uso, es decir funciones que el sistema no debe permitir que puedan resultar en pérdidas para la organización.

La creación de casos de abuso es un proceso de una lluvia de ideas apoyándose como entrada en documentación como casos de uso, patrones de ataque y requerimientos. Las actividades realizadas son identificar, documentar, examinar y revisar amenazas que den paso a la creación de requerimientos negativos y modelos de ataque, con en análisis y revisión de esta información genera como salida los documentos de casos de abuso.

El documento de casos de abuso debe contener condiciones iníciales, suposiciones, peor caso de amenaza, (post-condición), alcance y la meta del atacante.

Los requerimientos de seguridad que como mínimo deben cumplir los desarrolladores de las aplicaciones tomado como guía los estándares del de verificación de seguridad en aplicaciones de OWASP, para mitigar las vulnerabilidades identificadas con la metodología de análisis de riesgo propuesta son:

Administración de usuarios y autenticación

Las aplicaciones deben tener implementado funciones para la administración de usuarios y autenticación, de igual forma contar con un módulo de asignación de roles para cada uno de los usuario.

Requerimientos

- Para aplicaciones de uso interno la autenticación de los usuarios se debe realizar contra el LDAP, el cambio de contraseñas estará sometido a las políticas de cambio periódico de contraseña periódica implantada por la entidad.

- Para los servicios y aplicaciones expuestos a la ciudadanía se debe implementar un formulario de registro donde se solicite información básica (Nombre, Apellido, número de cédula y correo electrónico), las contraseñas deben cumplir con ciertas características de seguridad:

    - No menor a ocho caracteres.
    - Que contenga como mínimo una letra minúscula y una mayúscula.
    - Que contenga como mínimo un carácter especial.
    - El restablecimiento de contraseña se debe realizar por medio de preguntas de seguridad.

- No se concederán usuarios con privilegios de administrador para los accesos a los servidores, bases de datos, almacenamiento de las aplicaciones, para ninguno de los ambientes (Desarrollo, Pruebas y Producción).

- No se tendrán usuarios genéricos o administrados por varios desarrolladores o administradores de la plataforma tecnológica.

Autorización

La autorización permitirá determinar si conceden permisos a recursos o módulos de las aplicaciones, esta verificación sucede luego del proceso de autenticación, donde se determina quien tiene acceso a qué.

Requerimientos

- El mecanismo de control de acceso debe estar basado en el modelo de seguridad RBAC, que permite restringir las operaciones que puede realizar un usuario, mediante la definición de roles, permisos y la asignación de los mismos a los usuarios de la organización.

- El acceso a los módulos o funciones que realizará cada funcionario en las aplicaciones estará definido por un esquema de control de acceso por roles, de acuerdo al cargo y/o funciones se asignaran los permisos.

- La asignación de permisos a los módulos de la aplicación dependerá de las funciones a desempeñar por el funcionario y/o contratista previa a la autorización del jefe o superior.

- Asegurar que los usuarios autorizados tengan acceso a los recursos basándose en permisos asignados a los roles del usuario.

- Contar con una jerarquía de roles, que posibilita de una manera natural organizarlos para reflejar la organización de las empresas, para esto se basa en la relación de responsabilidad de los usuarios. Esto facilita significativamente la administración del sistema.

Manejo de sesiones

Las aplicaciones deben garantizar la comunicación de cliente-aplicación durante el período de tiempo que dure la sesión o transacción.

Requerimientos

- Las aplicaciones no permitirán tener dos sesiones simultáneas para un mismo usuario.

- La sesión debe tener un ID único aleatorio y estar cifrado, utilizando algoritmos criptográfico y enviadas por un canal seguro como el protocolo HTTPS. Una vez la sesión caduque o se cierre se debe generar un id nuevo para la nueva sesión.

- Asegurar que existan mecanismos que permitan verificar la auditoría de las transacciones y operaciones que realizó el usuario durante su sesión.

- Después de un tiempo determinado de inactividad, del usuario sobre la aplicación la sesión debe cerrarse.

- Debe existir la opción visible (salida segura) para que el usuario cierre su sesión.

- Cuando la aplicación se encuentre en clúster y uno de los nodos falle se debe garantizar que el usuario mantendrá su sesión con el ID asignado.

Validación de datos

Se debe garantizar la validación de los datos de entrada, en tal sentido es obligatorio realizar filtrado de los datos introducidos por el usuario a la aplicación.

Requerimientos

- Para evitar inyección de código maliciosos por Cross-Site Scripting se debe restringir y filtrar el uso de caracteres como <, >,',",(,),; y sus codificaciones (<, > , %60, %62,<, >) entre otras.

- Las aplicaciones deben tener comentarios o ventana emergentes que le indiquen al usuario que caracteres pueden o no utilizar, en los registros que realice.

- Garantizar que la aplicación no es susceptible a SQL injection.

- Implementar mecanismos de validación síncronos, es decir que el usuario tiene que corregir los datos erróneos antes de pasar al siguiente campo o transacción.

- Todas las fallas de validación de datos se registraran en los Logs de la aplicación.

Configuración de infraestructura

La incorrecta configuración de los recursos de infraestructura, donde se alojan las aplicaciones, genera lentitud, indisponibilidad, afectando el performance de las aplicaciones.

Requerimientos

- Las aplicaciones tendrán ambientes separados, como lo son Desarrollo, Pruebas y Producción.

- Los desarrolladores no tendrán acceso con usuario local a los servidores de los ambientes pruebas y producción.

- Los sistemas operativos a utilizar sobre los servidores deben contar con el soporte de licenciamiento o suscripción con el fabrícate, para el caso específico solo plataformas Windows y Linux Red Hat.

- La arquitectura de los desarrollo deben estar en lenguaje JAVA y utilizando plataforma Middleware Red Hat JBoss EAP.

Las actividades antes descritas, ayudan a definir el comportamiento del sistema para prevenir ataques e identificar riesgos a los cuales se les hará frente.

Fase de Análisis:

En esta fase se realiza la identificación de los riesgos claves relacionados con el activo, su arquitectura, sus amenazas, vulnerabilidades y controles, con base en la metodología de análisis de riesgos que fue definida en el presente trabajo.

IDENTIFICACIÓN Y ANÁLISIS DE LOS RIESGOS PROCESOS ETAPA PROCESAL - ADMINISTRAR RECURSOS INFORMÁTICOS					
Id Riesgo	**Activo de Información**	**Amenaza**	**Vulnerabilidad**	**Riesgo**	**Criterio**

Esta actividad entre otras, proporciona la información de las amenazas que pueden aprovechar vulnerabilidades de la arquitectura que se elija.

Fase de Codificación

La revisión de código fuente por otros desarrolladores se considerada la actividad más importante entre las mejores prácticas de seguridad que se deben realizar en el transcurso del desarrollo de una aplicación, es adecuado para identificar problemas de seguridad por las siguientes razones:

- Permite encontrar errores incluso antes del despliegue de la aplicación.
- Permite identificar la causa origen de un problema de seguridad.
- Necesidad de encontrar vulnerabilidades que puedan ser explotables.

Las herramientas de análisis estático de código son parte del proceso de revisión de código, ya que hacen que sea mucho más eficiente, se especifican debilidades aprovechadas por amenazas y las técnicas de desarrollo que permiten evitar los defectos.

Algunas de las herramientas recomendadas a utilizar por su capacidad para comprender los programas que se analizan, facilidad de usar, el conjunto de errores que comprueba, precisión, profundidad y la escalabilidad son las siguientes:

Comerciales

- SCA de Fortify software.
- AppScam.

Gratuitas

- OWASP SonarQube Project.
- OWASP Orizon Project.
- OWASP LAPSE Project.
- OWASP O2 Platform.
- OWASP WAP-Web Application Protection.

Fase de Pruebas

En esta fase se deben realizar actividades de escaneo de vulnerabilidades y pruebas de seguridad basadas en el riesgo.

Los objetivos de las pruebas de seguridad basadas en el riesgo son los siguientes:

- Verificar la operación confiable del software bajo condiciones hostiles de ataque.
- Verificar la fiabilidad del software, en términos de comportamiento seguro y cambios de estado confiables.
- Verificar la falta de defectos y debilidades explotables.

- Verificar la capacidad de supervivencia del software ante la aparición de anomalías, errores y el manejo de las mismas, mediante excepciones que minimicen el alcance e impacto de los daños que puedan resultar de los ataques.

Con el propósito de obtener el mínimo de características de seguridad en una aplicación web, se sugiere seguir las recomendaciones del Open Web Application Security Project (OWASP).

El OWASP publica cada cierto tiempo una lista con las vulnerabilidades más comunes de las aplicaciones web, su descripción y recomendaciones para dar manejo a dichas vulnerabilidades.

Para determinar qué tan segura es una aplicación web respecto a las vulnerabilidades anteriormente referenciadas, existen herramientas de software que permiten hacer un análisis de las aplicaciones web y reportar las posibles alertas de seguridad que esta presenta. En este caso, se hará una descripción del proceso mediante la herramienta gratuita desarrollada por OWASP y un equipo de voluntarios llamada ZedAttack Proxy (ZAP).

Descargar la herramienta ZAP

De la página de descargas se puede obtener la versión para Windows, Linux, Mac OS y Cross platform. En este caso se descarga la opción ‘Cross platform’ que no requiere instalación ni permisos de administrador.

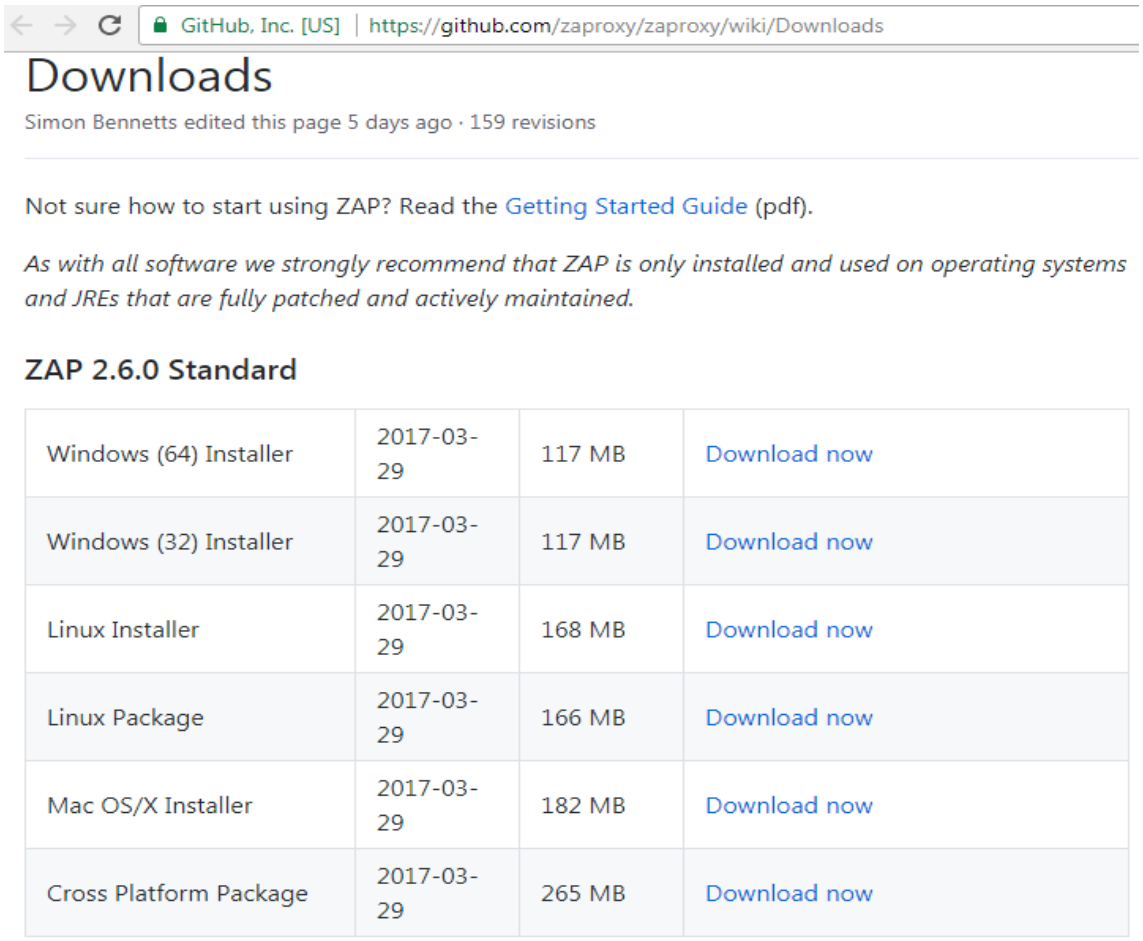


Ilustración 1 Repositorio Github de ZAP proxy

Ejecutar la herramienta ZAP

Luego de descargar el paquete ZAP_2.6.0_Cross_Platfom.zip para este caso, se procede a descomprimir el archivo y ubicar en la carpeta ZAP_2.6.0 el archivo 'zap.bat' o 'zap.sh' o el archivo ZAP_2.6.0.jar según el sistema operativo.

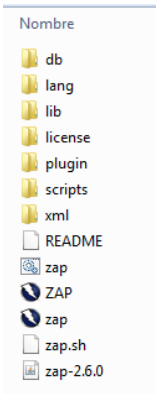


Ilustración 2 Archivo ejecutable

Al hacer ejecutar el archivo aparece la interfaz gráfica de la herramienta y se inicia el servicio en segundo plano.

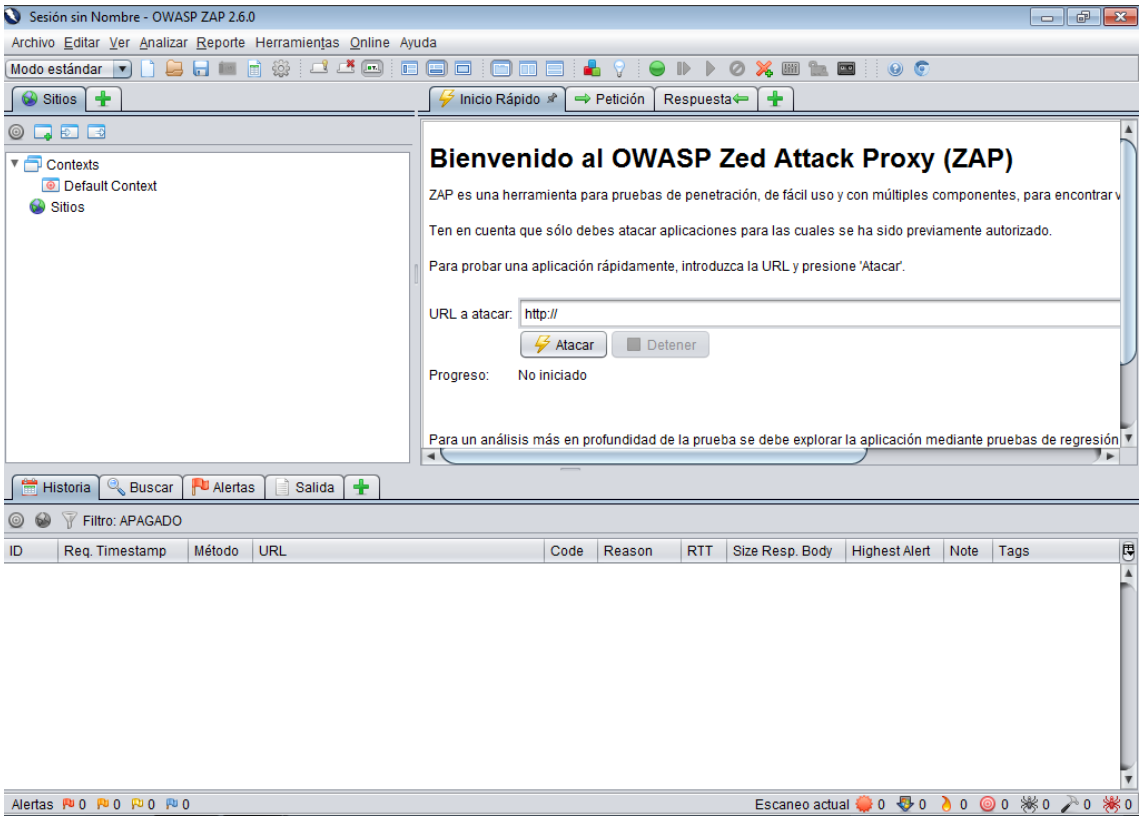


Ilustración 3 Interfaz gráfica

Reporte de alertas

Para ver el reporte de alertas detectadas por la herramienta ZAP en una aplicación web, basta con navegar por la aplicación, automáticamente aparecerán las alertas de cada ruta que se navegue sobre la interfaz gráfica de ZAP:

Ilustración 4 Reporte de alertas

Por cada ruta navegada aparece un registro con el nivel de alerta detectada. Sobre cada uno de los registros se puede hacer clic para ver el detalle del 'request HTTP' y 'response HTTP'. También se puede acceder a un menú contextual que aparece al hacer clic derecho, del cual destacan las opciones 'Atacar' y 'Alertas para este nodo':

Ilustración 5 HTTP Request (pestaña petición)

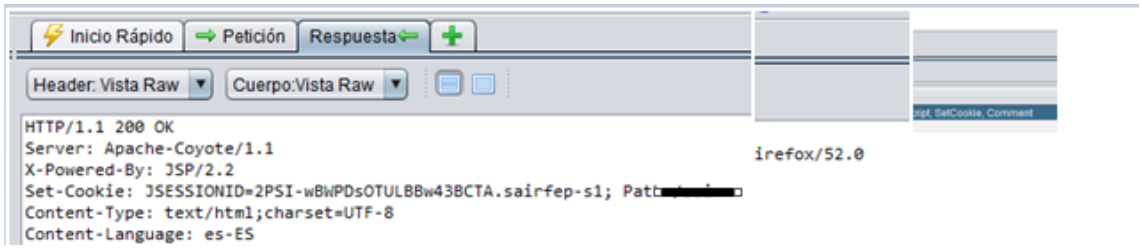


Ilustración 6 HTTP Response (pestaña respuesta)

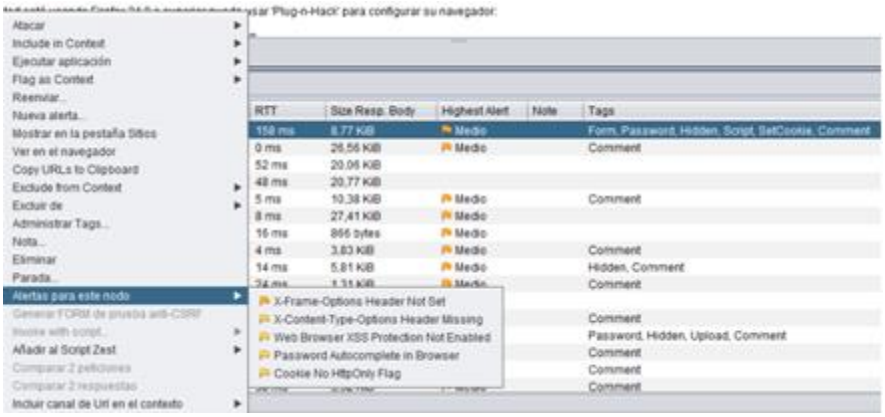


Ilustración 7 Menú contextual (clic derecho)

Por último, al elegir una de las alertas del menú contextual, aparece una ventana emergente con una descripción de la vulnerabilidad y unas URL que dirigen al sitio oficial de OWASP y de terceros con descripciones más detalladas e indicaciones sobre cómo mitigar el riesgo de seguridad asociado.

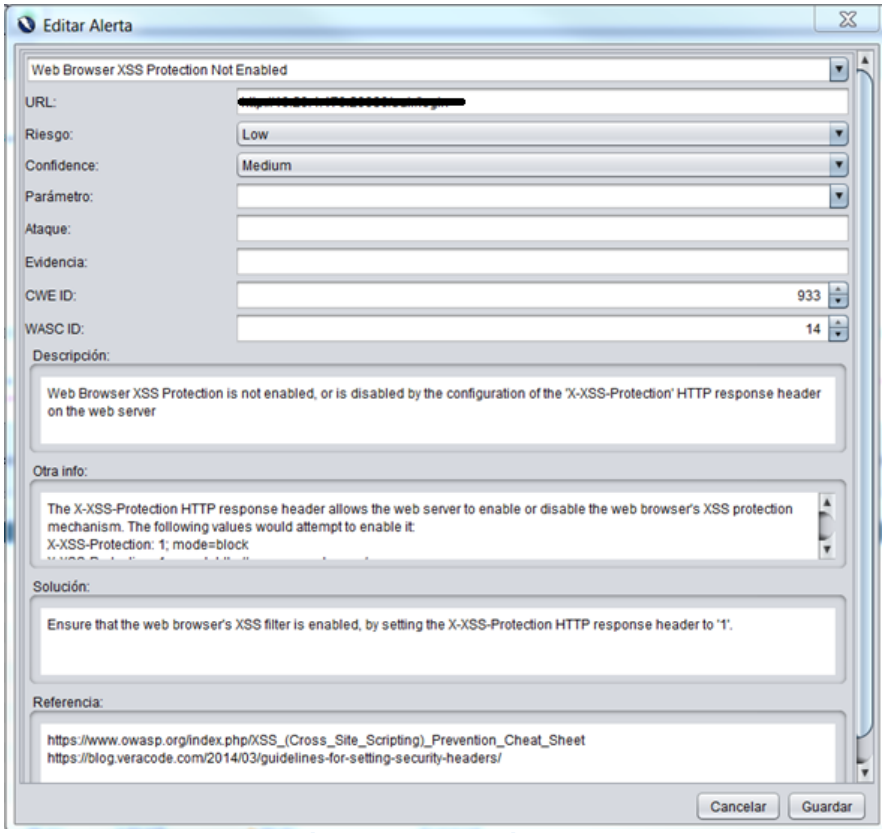


Ilustración 8 Descripción de la alerta

Fase publicación segura

Una de las actividades que se deben desarrollar son modelos de ataque, como mecanismo para entender la perspectiva de un ciberatacante para ello se presenta un modelo de formato que permita registrar el detalle de los ataques, los exploit más frecuentes y técnicas utilizadas para comprometer el software.

Ítem	Descripción
Nombre	Identificador del patrón de ataque.
Severidad	Escala de gravedad del ataque (bajo, medio, alto).
Descripción	Descripción detallada del ataque incluyendo el paso a paso de las acciones tomadas por el atacante, contiene casos demostrativos de ejemplo del ataque.
Prerrequisitos del ataque	Describe las condiciones y características que deben existir en el software destino para que el ataque sea exitoso.
Conocimientos y habilidades del atacante	Describe el conocimiento requerido y habilidades para poder ejecutar el ataque.
Soluciones y mitigaciones	Describe acciones que pueden prevenir o mitigar el riesgo de este tipo de ataques.
Impacto CID	Define el impacto del ataque en Confidencialidad, Integridad y Disponibilidad.
Vulnerabilidades relacionadas	Se indican las vulnerabilidades o debilidades que puede el ataque explotar.

La actividad descrita permitirá la selección de políticas y configuraciones acordes a las amenazas obtenidas en los modelos de ataque.