



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

**Ethical hacking aplicado al sistema de gestión
documental de la ONPE para evitar vulnerabilidades y
acceso no autorizado a la información**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Juan Carlos CALIXTO SALAZAR

ASESOR

Adegundo Mario CÁMARA FIGUEROA

Lima, Perú

2018



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Calixto, J. (2018). *Ethical hacking aplicado al sistema de gestión documental de la ONPE para evitar vulnerabilidades y acceso no autorizado a la información*. Trabajo de Suficiencia Profesional para optar el título de Ingeniero de Sistemas. Escuela Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú.

HOJA DE METADATOS COMPLEMENTARIOS

Código ORCID del autor	-
DNI o pasaporte del autor	44674075
Código ORCID del asesor	0000-0001-5635-7277
DNI o pasaporte del asesor	09095759
Grupo de investigación	NO
Agencia financiadora	NO
Ubicación geográfica donde se desarrolló la investigación	Oficina Nacional de Procesos Electorales, Jirón Washington 1894, Santa Beatriz, Lima, Perú Latitud: -12.063313 Longitud: -77.039081
Disciplinas OCDE	Ingeniería de sistemas y comunicaciones http://purl.org/pe-repo/ocde/ford#2.02.04



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
Escuela Profesional de Ingeniería de Sistemas

**Acta de Sustentación del
Trabajo de Suficiencia Profesional**

Siendo las ^{14:20}.....horas del día ²⁰.....de diciembre del año 2018, se reunieron los docentes designados como Miembros de Jurado del Trabajo de Suficiencia Profesional, presidido por el Ing. Machado Vicente Joel Fernando (Presidente), Mg. Guerra Grados Luis Ángel (Miembro) y el Ing. Cámara Figueroa Adegundo Mario (Miembro Asesor) para la sustentación del Trabajo de Suficiencia Profesional Intitulado: **"ETHICAL HACKING APLICADAS AL SISTEMA DE GESTION DOCUMENTAL DE LA ONPE PARA EVITAR VULNERABILIDADES Y ACCESO NO AUTORIZADO A LA INFORMACION"**, por el Bachiller: **Calixto Salazar, Juan Carlos**; para obtener el Título Profesional de Ingeniero de Sistemas.

Acto seguido de la exposición del Trabajo de Suficiencia Profesional, el Presidente invitó al Bachiller a dar las respuestas a las preguntas establecida por los miembros del Jurado.

El Bachiller en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros del Jurado, el Bachiller obtuvo la nota de 18.... (En letras) Dieciocho.....

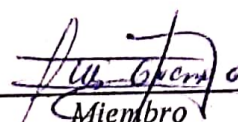
A continuación el presidente del jurado el Ing. Machado Vicente Joel Fernando, declara al Bachiller Ingeniero de Sistemas.

Siendo las ¹⁵.....horas, se levantó la sesión.



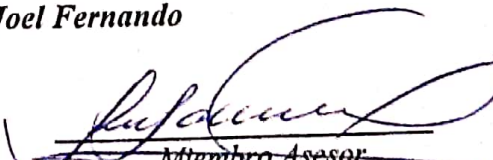
Presidente

Mg. Machado Vicente Joel Fernando



Miembro

Ing. Guerra Grados Luis Angel



Miembro Asesor

Ing. Cámara Figueroa Adegundo Mario

FICHA CATALOGRÁFICA

ETHICAL HACKING APLICADO AL SISTEMA DE GESTIÓN DOCUMENTAL DE LA ONPE PARA EVITAR VULNERABILIDADES Y ACCESO NO AUTORIZADO A LA INFORMACIÓN

AUTOR: CALIXTO SALAZAR JUAN CARLOS

ASESOR: CÁMARA FIGUEROA, ADEGUNDO MARIO

LIMA-PERU, **2018**

Título Profesional/Grado Académico: Título Profesional de Ingeniero de Sistemas

Área/Programa/Línea de Investigación: Ingenierías / Tecnología de la Información y Comunicación / Ingeniería de Software

Pregrado: Universidad Nacional Mayor de San Marcos – Facultad de Ingeniería de Sistemas e Informática – Escuela Profesional de Ingeniería de Sistemas

Formato 28 x 20 cm

Páginas: xi, 138

DEDICATORIA

La culminación de este informe de Suficiencia Profesional, está dedicado a mis papas, motores y motivos de mi vida. Gracias a sus consejos y educación he podido lograr mis objetivos. Su arduo trabajo y ejemplo han hecho que inspiren mi vida, no solo la mía, sino la de mis hermanos y familia en general. También quiero dedicar este trabajo a mi esposa, Milagros Aguado Berrio por su incondicional apoyo. Ella representa e inspira esfuerzo y dedicación en momentos difíciles de mi vida. A mi hija Dulce María que es mi inspiración para avanzar en la vida. A ellos este proyecto, sin su apoyo, no hubiese podido ser.

Calixto Salazar Juan Carlos

AGRADECIMIENTOS

En primer lugar, a Dios por todo lo que me ha dado en la vida; en segundo lugar, a cada uno de los que son parte de mi familia a mi padre Antonio Calixto Dávila, a mi madre Victoria Salazar Falcón, a mis hermanos, a mi esposa Milagros Aguado Berrio y no menos importante a mi hija Dulce María Marissa, que me alentaron con su alegría y buenos deseos, gracias también a mi asesor quien me ayudó en todo momento, Ing. Mario Cámara.

Calixto Salazar Juan Carlos

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Ethical Hacking aplicado al Sistema de Gestión Documental de la ONPE para evitar vulnerabilidades y acceso no autorizado a la información.

Autor: Calixto Salazar, Juan Carlos

Asesor: Cámara Figueroa, Adegundo Mario

Título: Trabajo de Suficiencia Profesional para optar el Título Profesional de Ingeniero de Sistemas

Fecha: Diciembre 2018

RESUMEN

El Sistema de Gestión Documental es una herramienta informática, desarrollada por la ONPE, que utiliza la tecnología de los Certificados Digitales, lo que permite optimizar los procesos de Gestión de Documentos Administrativos en la Entidad que lo implemente. Kunak Consulting, empresa dedicada a realizar servicios de Ethical Hacking, llevó a cabo un servicio de análisis de vulnerabilidades sobre el Sistema de Gestión Documental. Mediante este servicio se determinó el nivel de riesgo de seguridad que posee los elementos tecnológicos del sistema desde una perspectiva EXTERNA. Kunak Consulting generó recomendaciones a partir de los resultados obtenidos para corregir los problemas encontrados en el Sistema de Gestión Documental, estas recomendaciones fueron implementadas en el sistema, para ello se utilizó una metodología que es de propia autoría de la institución, está implementada a partir de un conjunto de buenas prácticas, está basada en la metodología Proceso Unificado de Desarrollo. Finalmente, la implementación de buenas prácticas en seguridad informática al Sistema de Gestión Documental permitió que se evite al acceso no autorizado a la información, así como prevenir ataques informáticos. Esto a su vez convierte al Sistema de Gestión Documental en un sistema fiable y seguro.

Palabras claves: Sistema de Gestión Documental, Certificados Digitales, Ethical Hacking, Análisis de Vulnerabilidades, Seguridad Informática, Perspectiva Externa, Proceso Unificado de Desarrollo.

MAJOR NATIONAL UNIVERSITY OF SAN MARCOS
FACULTY OF SYSTEMS AND COMPUTER ENGINEERING
PROFESSIONAL SCHOOL OF SYSTEMS ENGINEERING

**Ethical Hacking applied to the ONPE Documentary Management System to prevent
vulnerabilities and unauthorized access to information.**

Author: Calixto Salazar, Juan Carlos
Advisor: Cámara Figueroa, Adegundo Mario
Title: Professional Sufficiency Work Report for opt for the Professional Title
of Systems Engineer
Date: December 2018

ABSTRACT

The Document Management System is a computer tool, developed by the ONPE, which uses the Digital Certificates technology, which makes it possible to optimize the Administrative Documents Management processes in the Entity that implements it. Kunak Consulting, a company dedicated to perform Ethical Hacking services, carried out a vulnerability analysis service on the Document Management System. Through this service, the level of security risk that the technological elements of the system have from an EXTERNAL perspective was determined. Kunak Consulting generated recommendations based on the results obtained to correct the problems found in the Document Management System, these recommendations were implemented in the system, for this a methodology was used that is of the institution's own authorship, is designed from A set of good practices that have international acceptance is based on the Unified Development Process methodology. Finally, the implementation of good practices in computer security to the Document Management System allowed to avoid unauthorized access to information, as well as to prevent computer attacks. This in turn makes the Document Management System a reliable and secure system.

Key words: Document Management System, Digital Certificates, Ethical Hacking, Vulnerability Analysis, Information Security, External Perspective, Unified Development Process.

ÍNDICE

CARÁTULA EXTERNA	i
PÁGINA EN BLANCO	ii
CARÁTULA INTERNA	iii
FICHA CATALOGRÁFICA	iv
DEDICATORIA	v
AGRADECIMIENTOS	vi
RESUMEN	vii
ABSTRACT	viii
ÍNDICE	ix
ÍNDICE DE FIGURAS	xi
ÍNDICE DE TABLAS	xiii
INTRODUCCIÓN	1
CAPÍTULO I – TRAYECTORIA PROFESIONAL	3
CAPÍTULO II – CONTEXTO EN EL QUE SE DESARROLLO LA EXPERIENCIA	7
2.1 EMPRESA – ACTIVIDAD QUE REALIZA	7
2.2 VISIÓN	9
2.3 MISIÓN	9
2.4 ORGANIZACIÓN DE LA EMPRESA	10
2.5 ÁREA, CARGO Y FUNCIONES DESEMPEÑADAS	11
2.6 EXPERIENCIA PROFESIONAL REALIZADA EN LA ORGANIZACIÓN	11
CAPITULO III – ACTIVIDADES DESARROLLADAS	12
3.1 SITUACIÓN PROBLEMÁTICA	12
3.1.1 DEFINICIÓN DEL PROBLEMA	16
3.2 CAUSAS	17
3.3 SOLUCIÓN	18

3.3.1 OBJETIVOS	18
3.3.2 ALCANCE	19
3.3.3 ETAPAS Y METODOLOGÍAS	22
3.3.4 IMPLEMENTACIÓN DE LAS ÁREAS DE PROCESOS Y SUS BUENAS PRÁCTICAS	26
3.4 EVALUACIÓN ECONÓMICA	59
CAPÍTULO IV – REFLEXIÓN CRÍTICA DE LA EXPERIENCIA	61
4.1 APORTES EN EL ÁREA DE DESARROLLO Y RESPONSABILIDADES	61
CAPÍTULO V – CONCLUSIONES Y RECOMENDACIONES	62
5.1 CONCLUSIONES	62
5.2 RECOMENDACIONES	63
FUENTES DE INFORMACIÓN	64
GLOSARIO	65
ANEXOS	68

ÍNDICE DE FIGURAS

Figura 1: Organigrama de la ONPE	10
Figura 2: Categoría de Nivel de Riesgo.....	13
Figura 3: Diagrama Causa y Efecto	17
Figura 4: Ubicación geográfica de la oficina principal de la ONPE	21
Figura 5: Solicitud URL enviada al servidor de aplicaciones	30
Figura 6: Usuario con perfil BÁSICO, no cuenta con las opciones de perfil ADMINISTRADOR en el módulo de CONFIGURACION	31
Figura 7: Evidencia de acceso no autorizado a las opciones de perfil ADMINISTRADOR.	32
Figura 8: Envío de Request URL al servidor de aplicaciones, utilizando la herramienta HackBar. ...	32
Figura 9: Evidencia de acceso no autorizado a la opción buscar empleado, privilegio del perfil ADMINISTRADOR.....	33
Figura 10: Vulnerabilidad controlada.....	34
Figura 11: Manipulación de parámetros en la opción Editar Documentos.	36
Figura 12: Evidencia que el usuario RCHAM no tiene acceso al número de emisión 2600.	37
Figura 13: Evidencia de acceso NO autorizado a información a través de la manipulación de parámetros por el usuario RCHAM.....	38
Figura 14: Evidencia de acceso no autorizado a información a través de la manipulación de parámetros por el usuario RCHAM.....	38
Figura 15: Vulnerabilidad controlada.....	39
Figura 16: Evidencia de parámetros de envío sin encriptación en todas las opciones del sistema.	42
Figura 17: Evidencia de parámetros de envío sin encriptación en todas las opciones del sistema.	43
Figura 18: evidencia de parámetros de envío sin encriptación en todas las opciones del sistema.	44
Figura 19: Parámetros de envío encriptado.....	45
Figura 20: parámetros de envío encriptados.	46
Figura 21: Parámetros de envío enumerados.	47
Figura 22: Ejecución de la herramienta Audits del navegador Chrome.	49
Figura 23: Resultados de la ejecución de la herramienta Audits del navegador Chrome.....	50
Figura 24: Observación subsanada al realizar la actualización del jQuery.	51
Figura 25: Imagen Ampliada Observación subsanada al realizar la actualización del jQuery.	51
Figura 26: Usuario accediendo al sistema.....	52
Figura 27: Imagen Captcha Luego de ingresar erróneamente la contraseña.....	53
Figura 28: Usuario es bloqueado luego de ingresar erróneamente la contraseña y el Captcha.....	53

Figura 29: Evidencia enumeración de cuentas de usuarios en el sistema.....55

Figura 30: Evidencia enumeración de cuentas de usuarios en el sistema.....56

Figura 31: El atacante obtiene listado de Empleados.....56

Figura 32: Evidencia enumeración de cuentas de usuarios en el sistema.....57

Figura 33: Vulnerabilidad Controlada.....57

ÍNDICE DE TABLAS

Tabla 1: Lista de vulnerabilidades Identificadas en el Sistema de Gestión Documental	16
Tabla 2: Flujo de caja del proyecto	60

INTRODUCCIÓN

El Sistema de Gestión Documental es una herramienta informática desarrollada por la ONPE, utiliza la tecnología de los Certificados Digitales, lo que permite optimizar los procesos de Gestión de Documentos Administrativos en la Entidad que lo implemente. Elimina el uso del papel en la gestión documental.

En los últimos años ha existido un uso indebido de las tecnologías de la información y comunicación por gente experta en el tema con la intención de realizar ataques en contra de la integridad de los sistemas computacionales, estos ataques han causado no solo pérdidas económicas a una empresa sino también en un caso más grave la detención de personas inocentes víctimas de estos ataques informáticos, o también ya sea por el mal uso de los recursos informáticos como la web en donde se hacen presentes las redes sociales o el internet en general.

Kunak Consulting llevó a cabo un servicio de escaneo de vulnerabilidades y Ethical Hacking sobre el Sistema de Gestión Documental. Mediante este servicio se determinó el nivel de riesgo de seguridad que posee los elementos tecnológicos del sistema desde una perspectiva Externa. Se encontraron 10 vulnerabilidades, siendo la inadecuada gestión de privilegios la que obtuvo mayor puntuación estándar de vulnerabilidad (CVSS).

El Sistema de Gestión Documental a pesar de no haber sido expuesta a ningún ataque hasta el momento, es propenso a ser objetivo de ataque debido a ser una institución con manejo de base de datos de importante información, es por esta razón que se implementó buenas prácticas en seguridad informática.

El presente informe consta de 5 capítulos a continuación se describe:

En el CAPÍTULO I se describe la trayectoria profesional, la experiencia y aprendizaje obtenido.

En el CAPÍTULO II se describe a la Oficina Nacional de Procesos Electorales, su organigrama, la misión y visión, y los servicios brindados.

En el CAPÍTULO III se refiere a la implementación de buenas prácticas de seguridad informática aplicadas al Sistema de Gestión Documental de ONPE.

En El CAPÍTULO IV hace mención al aporte del autor, el desarrollo profesional que demandó, la experiencia y las capacitaciones requeridas.

En el CAPÍTULO V se detallan conclusiones y recomendaciones.

CAPÍTULO I – TRAYECTORIA PROFESIONAL

PRESENTACIÓN PROFESIONAL
Soy un profesional de la carrera de Ingeniería de Sistemas, con especialización en el desarrollo de sistemas web. Tengo amplia experiencia profesional en organismos públicos de reconocido nivel. La experiencia profesional se realiza en los siguientes aspectos: - Análisis, Diseño y Desarrollo de soluciones tecnológicas. - Modelamiento y Análisis de Datos. Dinámico con facilidad para trabajar en equipo, capaz de realizar con responsabilidad, criterio y creatividad los trabajos que se me encargan, cumpliendo los objetivos y metas trazadas

FORMACIÓN	
Educación Superior Grado académico de bachiller en ingeniería de sistemas (27-May-2016) Escuela académico profesional de ingeniería de sistemas Facultad de ingeniería de sistemas e informática Universidad Nacional Mayor de San Marcos	Abr.2007 – Jul.2015
Educación Secundaria I.E José Antonio Encinas	Año 2000 – Año 2003

EXPERIENCIA PROFESIONAL	
Oficina Nacional de Procesos Electorales • Cargo: Desarrollador de servicios web. • Principales funciones: ✓ Análisis, desarrollo e implementación del Sistema de Gestión Documental. ✓ Implementación de la firma y emisión de documentos masivamente en el Sistema de Gestión Documental. ✓ Implementación de buenas prácticas en seguridad informática aplicadas al Sistema de Gestión Documental. ✓ Apoyar en la gestión del proyecto, así como en la coordinación para la definición de alcance y reglas de negocio.	06.03.2018 – hasta la fecha
Ministerio de Educación – Unidad de Estadística • Cargo: Analista Programador.	08.08.2017 -

• Principales funciones: ✓ Desarrollar e implementar aplicaciones y servicios web con tecnología Java, AngularJS, para la difusión de la información de los censos escolares. ✓ Plantear acciones de actualización y operatividad del portal web ESCALE, para la difusión de la información estadística educativa. ✓ Implementación y desarrollo de Inteligencia de Negocios con la herramienta SSAS de SQL SERVER, para la explotación de los datos de los censos escolares.	28.02.2018
Pertel de Perú S.A.C • Cargo: Analista Programador. • Principales funciones: ✓ Mantenimiento a los diferentes sistemas contables, utilizando lenguaje de programación java web, framework spring, jsp, HTML, JavaScript. ✓ Base de datos Oracle 11g Creación de store procedures para las nuevas necesidades de manejo de la información dentro de la empresa.	01.03.2017 - 31.07.2017
Ministerio de educación – Programa Nacional de Becas y • Cargo: Analista Programador. • Principales funciones: ✓ Mantenimiento de la base de datos del portal institucional del PRONABEC. ✓ Desarrollo de efectos y animaciones para el nuevo portal institucional. ✓ Mantenimiento y actualizaciones al portal institucional. ✓ Implementación y desarrollo del sistema de gestión de contenido web OPC.	01.10.2016 - 28.02.2017
Registro Nacional de Identificación y Estado Civil • Cargo: Desarrollador de Servicios Web. • Principales funciones: ✓ Analizar y plantear soluciones a los requerimientos informáticos. Principalmente del Sistema de verificación Automática de Firmas y Adherentes. ✓ Levantar información, analizar, diseñar e implementar nuevos requerimientos y/o mantenimientos de los aplicativos. ✓ Uso de los framework JQuery, Bootstrap, CSS3, HTML5 en la capa de presentación. ✓ Elaboración de reportes con JasperReports.	30.09.2015 - 30.09.2016

✓ Desarrollo y mantenimiento de aplicaciones web en Java con los frameworks: Spring – Mybatis para la Capa de Persistencia. ✓ Mantenimiento de base de datos Oracle PLSQL.	
Banco de la Nación del Perú- Departamento de informática-Sección de Desarrollo-Operaciones Bancarias. • Cargo: Practicante. • Principales funciones: ✓ Desarrollo y mantenimiento de aplicaciones web en Java con los frameworks: Hibernate – Spring – JSF. ✓ Desarrollo de web Service Rest Full, para el uso interno con las aplicaciones en JAVA. ✓ Uso del framework JQuery en la capa de presentación. ✓ Mantenimiento al sistema BDUC (Base de Datos Única de Clientes).	21.02.2014 - 30.06.2015
Banco Central de Reserva del Perú- Departamento de Estadística y balanza de Pagos • Cargo: Practicante. • Principales funciones: ✓ Desarrollo e implementación de aplicaciones web en .Net ✓ Reportes Cristal Report. ✓ Automatización de tareas utilizando Macros en Excel.	01.01.2013- 26.04.2013

IDIOMAS	
Inglés – Nivel Básico Centro de Idiomas – UNMSM	May. 2007 – Jul.2007

CURSOS	
Java Web Avanzado • Lugar: TECSUP	Octubre 2017 – Diciembre 2017
Java Web • Lugar: Centro de Extensión y Proyección Social de la Universidad Nacional de Ingeniería.	Octubre 2014 – Noviembre 2014
Java Base de Datos	Setiembre 2014 – Octubre 2014

Lugar: Centro de Extensión y Proyección Social de la Universidad Nacional de Ingeniería.	
Java Developer Lugar: Centro de Extensión y Proyección Social de la Universidad Nacional de Ingeniería	Agosto 2014 – Setiembre 2014

OTROS CONOCIMIENTOS	
Lenguajes de Programación	✓ Java ✓ C++ ✓ php ✓ javascript ✓ jquery ✓ .NET
Sistemas Operativos	✓ Windows XP ✓ vista, 8
Manejadores de bases de Datos	✓ Oracle 11G ✓ MySql ✓ SQL Server
Herramientas Case	✓ Rational Rose ✓ Erwin
Otros :	✓ Oficce ✓ Bootstrap ✓ jasperReport

CAPÍTULO II – CONTEXTO EN EL QUE SE DESARROLLO LA EXPERIENCIA

2.1. EMPRESA – ACTIVIDAD QUE REALIZA

“La ONPE es el organismo electoral constitucional autónomo que forma parte del Estado. Es la autoridad máxima que se encarga de organizar y ejecutar distintos procesos electorales, de referéndum y otros tipos de consulta popular” (ONPE, 2007).

“ONPE brinda asistencia técnica en la elección de autoridades de centros poblados, de universidades, de representantes de la sociedad civil a nivel nacional y local, en los consejos de coordinación regional y local” (ONPE, 2007).

“La entidad promueve la cultura electoral democrática, el respeto de los derechos políticos de la mujer en cumplimiento a la política de igualdad de oportunidades entre hombres y mujeres y otras que las leyes señalan” (ONPE, 2007).

“De igual modo, desarrolla la investigación electoral mediante la producción de documentos de información sistematizada de los procesos electorales y de consulta realizados” (ONPE, 2007).

Datos de Empresa: Razón Social: Oficina Nacional de Procesos Electorales.

Domicilio Legal: Jr. Washington 1894, Cercado de Lima – Lima-Perú.

Teléfono: (01) 4170630

RUC: 20291973851

Principales Convenios

La Oficina Nacional de Procesos Electorales ofrece asistencia técnica a 60 entidades del estado entre las que destacan:

- Oficina de Normalización Profesional.
- Ministerio de Educación.
- Universidad Nacional Mayor de San Marcos.
- Ministerio de Desarrollo e Inclusión Social.
- Biblioteca Nacional.
- Superintendencia Nacional de Migraciones.
- Programa Juntos.
- Programa Pensión 65
- Fuerza Aérea del Perú.

Principales Proveedores:

- MICROSOFT
- LENOVO
- CISCO
- ORACLE

Mercado:

La participación de la ONPE se da a través de convenios interinstitucionales, asistencia técnica, verificación de firmas y venta de kits electorales, beneficiando a muchas instituciones del estado y principalmente al ciudadano (ONPE, 2007).

Productos y/o Servicios:

- Asistencia Técnica.
- Verificación de Firmas.
- Trámites y Constancias.
- Venta de Kits.
- Verificación en Documentos Electorales.
- Supervisión del financiamiento de las organizaciones políticas.

2.2. VISIÓN

“Ser una institución de excelencia que cuenta con la confianza de la población, promoviendo una cultura de valores democráticos mediante el uso de tecnología e innovación” (ONPE, 2007).

2.3. MISIÓN

“Velar por la obtención de la fiel y libre expresión de la voluntad popular de los ciudadanos, organizaciones políticas, instituciones públicas, privadas y de la sociedad civil, en todos los procesos electorales” (ONPE, 2007).

2.4. ORGANIZACIÓN DE LA EMPRESA

Se muestra el Organigrama de cómo está organizado La Oficina Nacional de Procesos electorales ONPE correspondiente al actual periodo de funcionamiento

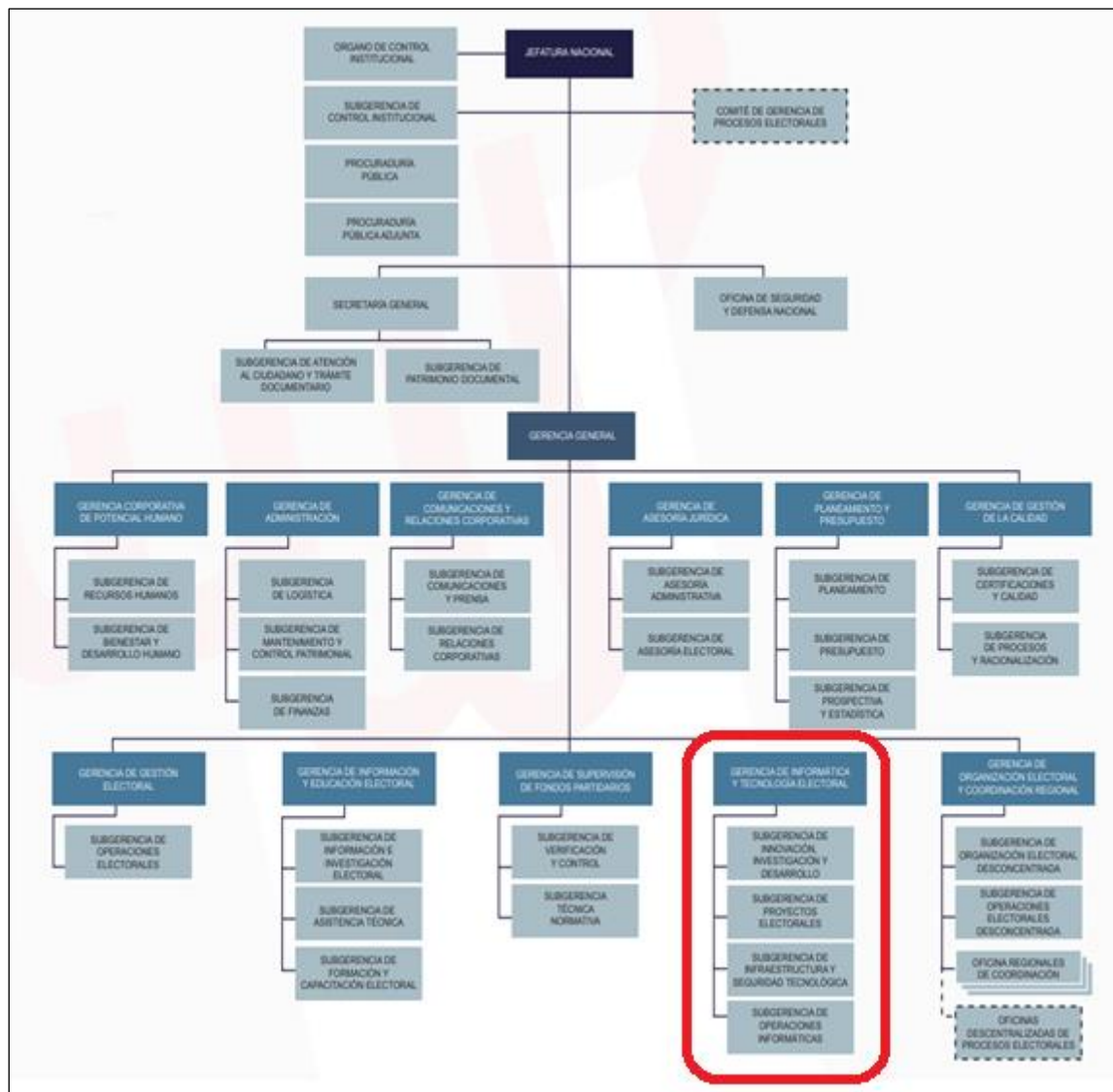


Figura 1: Organigrama de la ONPE

2.5. AREA CARGO Y FUNCIONES DESEMPEÑADAS

EL autor del presente informe se desempeña como Analista Programador en la Sub Gerencia de Ingeniería de Software que pertenece a la Gerencia de Tecnología de la Información, esta área constituyo el equipo de desarrollo e implantación del Sistema de Gestión Documental supervisada la Secretaría General de la ONPE.

2.6. EXPERIENCIA PROFESIONAL REALIZADA EN LA ORGANIZACIÓN

Funciones realizadas:

- Levantar la información acerca de los procesos asignados.
- Implementar módulos de los sistemas a cargo.
- Elaborar pruebas de flujo, para pruebas internas de los módulos de los sistemas a cargo.
- Realizar el análisis de las funcionalidades a desarrollarse, a su vez asegurar el correcto funcionamiento de los módulos a cargo.
- Realizar la subsanación de las observaciones realizadas por el área de aseguramiento de control de la calidad.

Apoyar en la gestión del proyecto, así como en la coordinación para la definición de alcance y reglas de negocio.

- Apoyar en la elaboración de la documentación requerida, la que incluye: manual de usuario, la que incluye manual de usuario, manual de instalaciones y documentos de tecnologías de la información que sean asignados.
- Apoyar en el análisis y elaboración de los diseños físicos y/o diseños lógicos de los módulos de los sistemas asignados.
- Apoyar en la elaboración de la arquitectura de software de los sistemas asignados.

CAPÍTULO III - ACTIVIDADES DESARROLLADAS

Durante el año 2018, periodo en el que se implementó buenas prácticas en seguridad informática al Sistema de Gestión Documental, fue necesario realizar las siguientes actividades:

- Reuniones con el personal encargado del Sistema de Gestión Documental.
- Definir el problema y analizar sus detalles.
- Validar accesos por roles y privilegios a las diferentes opciones que cuentan los usuarios del Sistema del Gestión Documental.
- Validar y restringir el acceso al detalle de los documentos administrativos, personales y de Mesa de Partes a aquellos usuarios que intenten acceder y/o modificar información que no le corresponda.
- Implementar la encriptación de parámetros enviados por URL al servidor de aplicaciones.
- Implementar librería de imagen Captcha.
- Modificar lógica de programación de acceso al Sistema de Gestión Documental.
- Modificar a nivel de programación la estructura de las respuestas de cabeceras de todas las páginas que componen el sistema.

3.1. SITUACIÓN PROBLEMÁTICA

En el año 2017, La Oficina Nacional de Procesos electorales contrató los servicios de la empresa Kunak Consulting para identificar las distintas vulnerabilidades que podría presentar el Sistema de Gestión Documental. La empresa Kunak Consulting trajo consigo la identificación de un conjunto de vulnerabilidades calificadas según el nivel de riesgo que presentan (kunak, 2017), las cuales se dividen en:

Leyenda de los riesgos identificados			
Categoría	Alto	Medio	Bajo
Nivel de riesgo			

Figura 2: Categoría de Nivel de Riesgo

Vulnerabilidad Alta: en esta clasificación se encuentran las vulnerabilidades que son ampliamente explotadas, que tienen herramientas de explotación conocidas y ampliamente difundidas y en algunos casos estas no requieren de un gran conocimiento para su uso, incluyendo también virus, gusanos o troyanos. Constituyen un compromiso total del sistema o una segura negación de servicio. Se incluyen aquí instalaciones por defecto con usuarios de altos privilegios con contraseñas débiles o sin ellas.

Vulnerabilidades Altas encontradas en el sistema SGD:

- Inadecuada gestión de privilegios: Acceso no autorizado a las opciones del perfil Administrador**

Se identificó que los usuarios que no cuentan con privilegios de administrador, pueden acceder a opciones de dicha sección.
- Inadecuada gestión de privilegios: Acceso no autorizado al detalle de documentos emitidos/recepcionados por usuarios (sección Consultas)**

Se identificó que usuarios que no cuentan con permisos para listar y observar el detalle de documentos emitidos pueden acceder a estos a través de la manipulación de parámetros.
- Inadecuada Gestión de Privilegios: Acceso no autorizado al detalle de documentos emitidos/recepcionados por usuarios (sección Documentos)**

Se identificó que los usuarios que no cuentan con permisos para listar y observar el

detalle de documentos emitidos pueden acceder a estos a través de la manipulación de parámetros.

- **Inadecuada Gestión de Privilegios: Acceso no autorizado al detalle de documentos recepcionados por usuarios (sección Mesa de Partes)**

Se identificó que los usuarios que no cuentan con permisos para listar y observar el detalle de documentos recepcionados pueden acceder a estos a través de la manipulación de parámetros.

- **Inadecuada Gestión de Privilegios: Recepción de documentos de manera no autorizada**

Se identificó que usuarios que no cuentan con permisos para recepcionar documentos pueden hacerlo suplantando la identidad de otros usuarios.

- **Inadecuada Gestión de Privilegios: carga/modificación de documentos de manera no autorizada.**

Se identificó que a través de la modificación de parámetros es posible cargar y/o modificar documentos asociados a documentos emitidos.

Vulnerabilidad Media: Aquí entran todas aquellas vulnerabilidades que no comprometen la integridad del sistema directamente o que no se conocen herramientas que puedan explotar aún estas vulnerabilidades. Constituyen un paso medio en el proceso de ataque. Permiten fugas de información para ataques más elaborados o defectos menores de sistema o de implementación que afectan el rendimiento o uso normal del sistema sin causar una negación de servicio.

Vulnerabilidades Medias encontradas en el sistema SGD:

- **Formulario de acceso al sistema susceptible a ataques recurrentes de acceso**

Se identificó que el formulario de acceso cuente con controles débiles que prevengan ataques recurrentes de acceso NO autorizado.

- **Formulario de acceso permite la enumeración de usuarios del sistema de**

información

Se identificó que el formulario de acceso al sistema de información permite obtener identificar si un usuario se encuentra registrado en el mismo.

- **Identificación de información innecesaria transferida en las solicitudes enviadas en el sistema de información.**

Se identificó que la solicitud de acceso al sistema transfiere información innecesaria que puede ser utilizada por un eventual atacante para realizar ataques.

Vulnerabilidad Baja: En esta categoría se encuentran las vulnerabilidades que apenas pueden considerarse como peligrosas. Constituyen pequeñas fugas de información de sistema, comportamientos que permiten mapeo de la red o simplemente saber si el sistema se encuentra activo. Se consideran vulnerabilidades porque con el tiempo si no son atendidas sirven como medio para ataques más elaborados. No se conocen herramientas especiales para su explotación, simplemente su funcionamiento normal genera estos pequeños defectos.

Vulnerabilidad Baja encontrada en el sistema SGD:

- **Debilidades en las cabeceras del protocolo HTTP**

Se identificó que las cabeceras del protocolo HTTP no cuentan con controles para prevenir ataques del tipo XSS y además expone información innecesaria.

3.1.1 DEFINICIÓN DEL PROBLEMA

El Sistema de Gestión Documental de la ONPE no contaba con buenas prácticas en seguridad informática. Esto debido a que la seguridad no fue prioritario en los requerimientos no funcionales del sistema, producto de ello el sistema estaba expuesto a ataques informáticos, específicamente en las siguientes vulnerabilidades:

Tipo	Descripción
Manipulación de parámetros.	Tiene por objetivo obtener acceso y/o modificar solicitudes (Request) del sistema de información para acceder a secciones restringidas o realizar operaciones sobre el sistema de información.
Ataques de inyección de scripts (XSS).	Tiene por objetivo, lograr inyectar código malicioso JavaScript, HTML etc. Cuya finalidad es engañar al usuario para suplantarlo.
Ataques de inyección de código (Inyección SQL).	Un ataque por inyección de código se aprovecha de la sintaxis del lenguaje para introducir comandos de manera ilícita que permitan leer o modificar la base de datos, comprometiendo el contenido de la consulta original.
Ataques de violación del protocolo HTTP.	Consiste en ataques a través de peticiones mal formadas que suelen acompañarse de intentos de ataques.
Ataques de acceso recurrente	Consiste en ataques de fuerza bruta de manera indeterminada, ataques de diccionario en base a patrones de contraseñas.

Tabla 1: Lista de vulnerabilidades.

3.2. CAUSAS

- Errores de diseño y programación; Los diseños, arquitecturas y/o soluciones no fueron consideradas para verificar las seguridades tanto en el lado del cliente como del servidor.
- Ausencia de personal especializado en Seguridad Informática en el área de calidad del software para las pruebas de Ethical Hacking a los sistemas informáticos de la institución.
- Ausencia de herramientas informáticas que permitan monitorear las vulnerabilidades del sistema de gestión documental.
- Prioridad a los requerimientos funcionales del sistema.
- No considerar pruebas de Ethical hacking a los Sistemas de Información de la institución

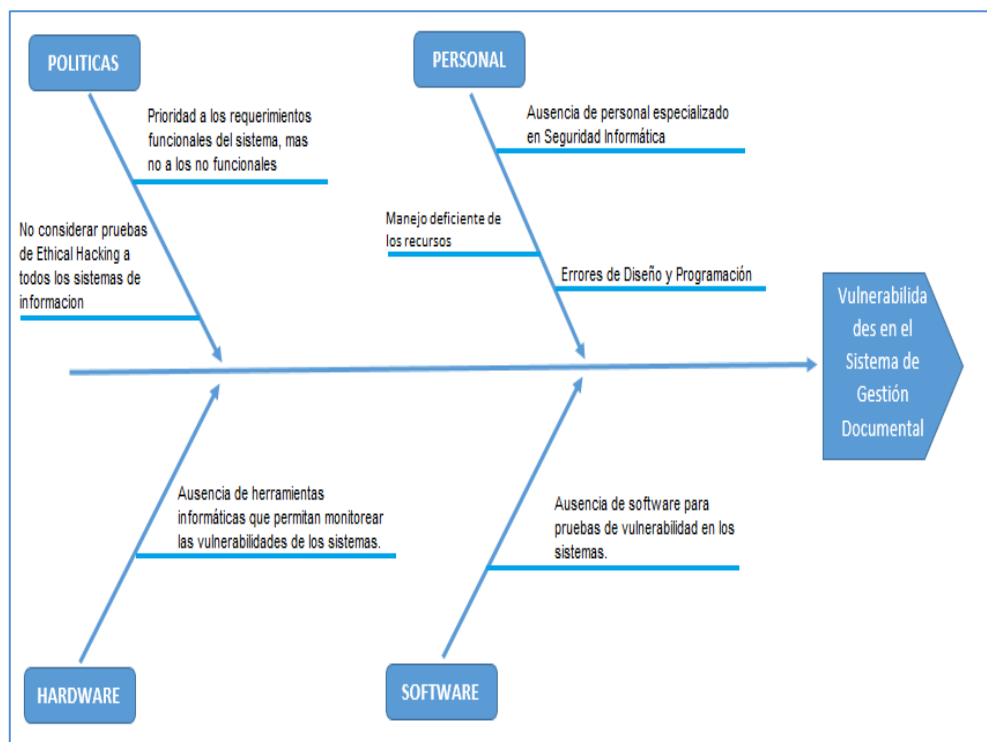


Figura 3: Diagrama Causa y Efecto

3.3. SOLUCIÓN

3.3.1 OBJETIVOS

OBJETIVO GENERAL

- Implementar Ethical hacking aplicado al Sistema de Gestión Documental de la ONPE para evitar vulnerabilidades y acceso no autorizado a la información.

OBJETIVOS ESPECÍFICOS

- Validar accesos por roles y privilegios a las diferentes opciones que cuentan los usuarios del Sistema de Gestión Documental.
- Evitar manipulación de parámetros mediante la transferencia de información a través de la encriptación de parámetros en el envío de las peticiones.
- Implementar librería de imagen Captcha.
- Modificar la lógica de programación de acceso al Sistema de Gestión Documental.
- Modificar a nivel de programación la estructura de las respuestas de cabeceras de todas las páginas que componen el sistema.
- Validar y restringir el acceso al detalle de los documentos administrativos, personales y de Mesa de Partes a aquellos usuarios que intenten acceder a información que no le corresponda.

3.3.2 ALCANCE

ALCANCE FUNCIONAL

La implementación de buenas prácticas en seguridad informática aplicadas al sistema de gestión documental, cubre todas las funciones correspondientes a los procesos de configuración, emisión y recepción de documentos y consultas. Contempla los siguientes módulos:

A. Módulo Configuración

- Configuración personal
- Registro de otros orígenes
- Registro de personas jurídicas
- Registro TUPA
- Registro de ciudadanos
- Registro de tipos de documentos por dependencia
- Registro de motivos de documentos por dependencias
- Registro de grupo destinos
- Acceso a la información
- Acceso a permisos
- Administración de unidades orgánicas
- Administración de funcionarios
- Administración de empleados
- Registro de requisitos
- Administración de perfiles

B. Módulo Documentos

- Emisión de documentos
- Recepción de documentos
- Emisión personal

C. Módulo Mesa de Partes

- Recepción de documentos externos
- Cargo de entrega
- Consulta documentos externos
- Seguimientos de documentos externos

D. Módulo Consulta

- Documentos emitidos
- Documentos recibidos
- Documentos visto bueno
- Documentos personales
- Seguimientos de emitidos
- Seguimientos de recibidos

ALCANCE ORGANIZACIONAL

El Sistema de Gestión Documental es utilizado en todas las dependencias de la institución a través de un entorno web; asegurando su difusión en todas las áreas de la institución donde se cuenta con conexión a internet.

ALCANCE GEOGRÁFICO

El alcance del Sistema de Gestión Documental abarca todas las dependencias de la Oficina Nacional de Procesos, así como las oficinas descentralizadas respectivas y las instituciones que bajo convenios interinstitucionales hacen uso del Sistema de Gestión Documental la ONPE (ONPE, 2007).

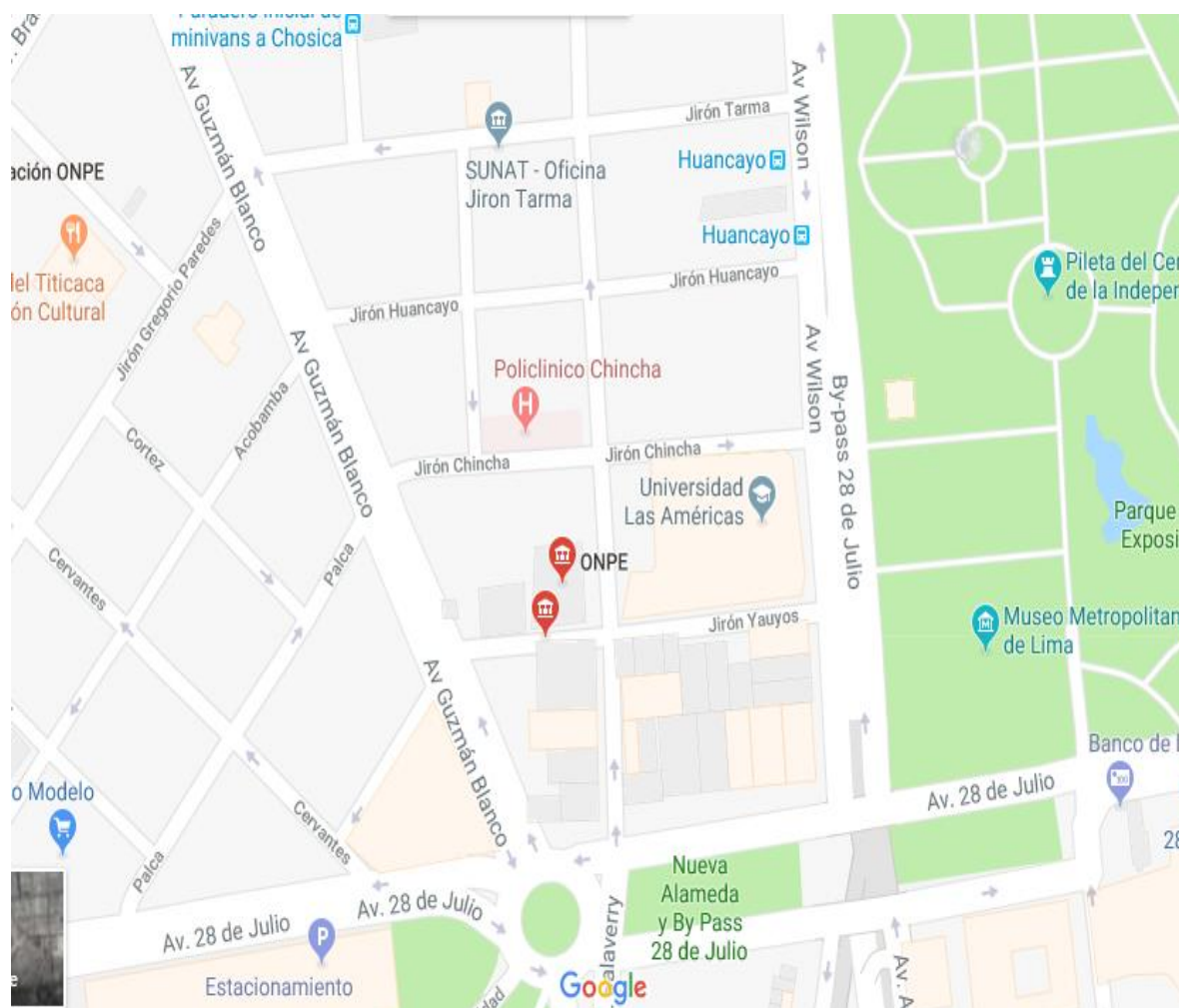


Figura 4: Ubicación geográfica de la oficina principal de la ONPE

3.3.3 ETAPAS Y METODOLOGIA

Metodología para el desarrollo de sistemas de información

Es el conjunto de tareas para implementar un sistema de información. Los objetivos de las metodologías del desarrollo de sistemas de información son:

- ✓ Concretar actividades a ejecutarse en un proyecto de sistema de información.
- ✓ Agrupar criterios en las organizaciones para el desarrollo de sistemas de información.
- ✓ Facilitar puntos de control de revisión.

La metodología utilizada para la gestión y desarrollo de los productos de software en la Oficina Nacional de Procesos Electorales es de propia autoría de la Institución, está diseñada a partir de un conjunto de buenas prácticas que tienen aceptación internacional alineada a estándares como la NTP-ISO/IEC 12207:2006 Tecnología de la Información Procesos del ciclo de vida del software (NTP ISO/IEC 12207, 2011), NTP-ISO/IEC 15504 Tecnología de Información: Evaluación de procesos (NTP ISO/IEC 15504, 2012) e ISO/IEC 24774 Life cycle management - Guidelines for process description (IEEE 24774-2012, 2012), ISO/IEC 12119 Information Technology Software Packages - Quality Requirements and Testing y contextualizada a la organización.

Esta misma metodología ha sido utilizada para la implementación de buenas prácticas en seguridad informática aplicadas al Sistema de Gestión Documental.

Está basada en la metodología Proceso Unificado de Desarrollo y cuenta con 7 Fases:

- ✓ Requerimiento
- ✓ Gestión.
- ✓ Viabilidad.
- ✓ Análisis.
- ✓ Diseño.
- ✓ Construcción.
- ✓ Implantación

Cada fase se define por separado, no se efectúan como gestiones aisladas.

Fase I: Requerimiento

En esta fase se realiza la toma de conocimiento y recojo de las necesidades del cliente y el usuario. Qué es lo que desea que el software realice. Hay que tener muy en cuenta que existen requerimientos funcionales y no funcionales.

.

Fase II: Gestión

Es la fase donde se establece formalmente el proyecto y los documentos y controles para gestionarlos durante su ejecución, se elabora el acta de constitución, matriz de interesados, documento de requisitos y plan de dirección. En esta etapa el analista se encarga de comprender la información y los datos derivados que requieren los interesados para llevar a cabo sus actividades.

En resumen comprende:

- ✓ Identificar a los involucrados, reglas y restricciones del negocio.
- ✓ Definir tiempos.
- ✓ Crear una estructura de desglose de trabajo.
- ✓ Recoger información acerca de los procedimientos y actividades que se desempeñan en la actualidad.

Fase III: Viabilidad

En esta fase el analista verifica la viabilidad y factibilidad del producto final del proyecto, se analiza la solicitud del usuario, el alcance del sistema, la viabilidad del sistema y el estudio de la situación actual de los procesos de negocios.

En resumen comprende:

- ✓ Identificar las limitaciones, restricciones y supuestos.
- ✓ Detectar las oportunidades.
- ✓ Analizar el modo actual de funcionamiento de la organización.
- ✓ Definir los requisitos que configuran el proyecto.
- ✓ Evaluar las distintas alternativas.
- ✓ Llegar a un acuerdo sobre la línea de acción.

Fase IV: Análisis

En esta fase el analista realiza el análisis del sistema, el análisis y comprensión del proceso involucrado, la recopilación de información principalmente de los usuarios interesados del sistema, se realizan tareas tales como, creación de prototipos, definición de módulos del sistema, documento de análisis, plan de pruebas y casos de pruebas del sistema

En resumen comprende:

- ✓ Recopilar información de los usuarios.
- ✓ Crear prototipos.
- ✓ Definir los módulos del sistema.
- ✓ Elaborar diccionario de datos y sus especificaciones.

Fase V: Diseño

En esta fase el analista realiza el diseño del sistema en general, plasma de manera mucho más concreta lo recopilado en la fase de análisis, genera soluciones a los requerimientos planteados, realiza el diseño físico y lógico, es decir resume como se va realizar el sistema.

En resumen comprende:

- ✓ Transformar los requerimientos al diseño del sistema.
- ✓ Definir la arquitectura tecnológica, de datos y funcional.
- ✓ Definir los patrones de diseño.
- ✓ Adaptar el diseño para que sea consistente con el entorno de implementación y ajustarla para un desempeño esperado.

Fase VI: Construcción

En esta fase se construye el sistema a partir del análisis y diseño, se crean el soporte lógico de datos (tablas, consultas, store procedures), se codifica el sistema en el lenguaje de programación elegido, utilizando patrones de diseño, se realiza Testing, etc., buscando satisfacer las necesidades del usuario mediante el cumplimiento de los requerimientos especificados.

En resumen comprende:

- ✓ Elaborar demostraciones para los usuarios y la interacción con las distintas interfaces.
- ✓ Elaborar actualizaciones para los diferentes procedimientos.
- ✓ Elaborar un informe con el tiempo que se llevó construir cada procedimiento.

Fase VII: Implantación

En esta fase se verifica la operatividad del sistema, se realizan las pruebas pertinentes por el área de calidad de software (QA), se pone en funcionamiento el sistema (puesta en marcha en producción), se capacitan a los usuarios finales, se entregan los manuales de usuario y se da la conformidad final de aprobación del sistema por parte de las área involucradas en el requerimiento.

En resumen comprende:

- ✓ Realizar el cronograma de las pruebas del software.
- ✓ El testeador deberá ejecutar un informe de sus tareas y pruebas para debatirlo con el desarrollador.

3.3.4 IMPLEMENTACION DE LAS AREAS DE PROCESOS Y SUS BUENAS PRACTICAS

Aplicando la metodología de ciclo de vida de un sistema según la metodología de ONPE, desarrollamos 7 pasos:

En la fase: Requerimiento

La identificación de vulnerabilidades al Sistema de Gestión Documental incluyó la revisión de configuraciones en relación a las buenas prácticas de programación, falta de actualización del software utilizado, uso de configuraciones por defecto, configuraciones débiles o erróneas, entre otras vulnerabilidades técnicas. Finalmente se generaron recomendaciones a partir de los resultados obtenidos para corregir los problemas encontrados.

La Gerencia de Informática de la ONPE determinó que las recomendaciones realizadas por la empresa Kunak Consulting sean tomadas como nuevos requerimientos a implementarse al

Sistema de Gestión Documental.

Listado de requerimientos a implementarse:

- a. Validar accesos por roles y privilegios a las diferentes opciones que cuentan los usuarios del Sistema de Gestión Documental.
- b. Validar y restringir el acceso al detalle de los documentos administrativos, personales y de mesa de partes a aquellos usuarios que intenten acceder y/o modificar información restringida.
- c. Implementar la encriptación de parámetros enviados por URL al servidor de aplicaciones.
- d. Implementar librería propia de imagen Captcha.
- e. Realizar cambio a nivel de lógica de programación del sistema sobre el formulario de acceso al sistema.
- f. Realizar la actualización de la versión de la biblioteca multiplataforma jQuery.
- g. Modificar a nivel de programación la estructura de las respuestas de cabeceras de todas las páginas que componen al Sistema de Gestión Documental.

En la fase: Gestión

En esta fase se realizaron una serie de reuniones con los encargados de la Sub Gerencia de Proyectos Electorales, Equipo de Infraestructura y Redes, Equipo de Aseguramiento de la Calidad y con el Líder Usuario del Sistema de Gestión Documental, con el propósito de definir el cronograma de actividades a realizarse en el presente proyecto. Se estimó que este trabajo tendría una duración aproximada de 5 meses.

En la fase: Viabilidad

En esta fase se analizaron las dos fases anteriores con la finalidad de determinar si los requerimientos eran factibles a realizarse. Se concluyó que los 10 requerimientos, organizados por nivel de vulnerabilidad, eran factibles.

El alcance de la implementación de Buenas Prácticas en Seguridad Informática aplicadas al Sistema de Gestión Documental abarca todas las opciones de todos sus módulos:

- ✓ Módulo Configuración
- ✓ Módulo Documentos
- ✓ Módulo Mesa de Partes
- ✓ Módulo Consultas

En las fases: Análisis y Diseño

Se evaluaron las 2 fases anteriores y en el Análisis se realizaron las siguientes actividades:

Se realizó la actualización del documento Especificación de Requerimientos del Software (ERS-415). Este documento tiene como finalidad brindar una guía fácil y de rápido entendimiento para las áreas usuarias, describiendo las funciones a ser implementadas en el Mantenimiento al Sistema de Gestión Documental.

A su vez se realizó la actualización del documento Reglas de Negocio (RN-415). Este documento tiene como objetivo identificar y especificar detalladamente las reglas del negocio definidas en el desarrollo del Mantenimiento del Sistema de Gestión Documental. Las reglas deben permitir identificar las condiciones de operación de cada una de las opciones implementadas en el sistema.

En la fase: Construcción.

Se describe las especificaciones técnicas de requerimientos que se utilizaron para implementar buenas prácticas en Seguridad Informática al Sistema de Gestión Documental.

1. Validar accesos por roles y privilegios a las diferentes opciones que cuentan los usuarios del Sistema de Gestión Documental.

En las recomendaciones brindadas en el informe técnico por la empresa Kunak Consulting, se sugiere la creación de una tabla de roles y privilegios en donde se especifique las opciones a las que debe tener acceso los usuarios del sistema de información, el Sistema de Gestión Documental ya contaba con una serie de tablas para dicho fin, pero no se estaba utilizando adecuadamente.

Para ello se implementó validaciones de acceso en la capa de control (Controller), de esta manera cuando un usuario intente acceder a una opción del sistema se realiza la consulta con las tablas correspondientes y evalúa si tiene privilegios para acceder al mismo.

Inicialmente durante el proceso de evaluación e identificación de vulnerabilidades, se realizaron pruebas de acceso no autorizado a secciones restringidas que son privilegiadas debido a la criticidad de las opciones que representan para el sistema de información. De manera puntual se realizaron pruebas de acceso a las opciones del perfil ADMINISTRADOR con usuarios que no cuentan con dicho privilegio.

El proceso de identificación de vulnerabilidades consistió en los siguientes pasos:

1. Se ingresa con el usuario JCALIXTO, este usuario tiene el perfil: Administrador
2. El usuario JCALIXTO cuenta con la opción CONFIGURACIÓN en el MENÚ de opción principal.
3. La opción CONFIGURACIÓN cuenta con opciones designadas solo al perfil Administrador y que no pueden ser accedidas/ejecutadas por perfiles que no cuenten con dicho perfil.

Para probar la vulnerabilidad se realizó lo siguiente:

4. Se ingresa con el usuario RCHAM este usuario tiene el perfil: Básico
5. Este usuario no cuenta con privilegios a la opción CONFIGURACIÓN.
6. Sin embargo, si el usuario RCHAM ejecuta directamente los enlaces asociados al perfil Administrador las páginas pueden ser accedidas/ejecutadas debido a que no se valida los accesos a las páginas.

Para el ejemplo el usuario RCHAM accedió a la siguiente dirección URL:

```
https://sisadm.onpe.gob.pe/sgd/1.0/srTablaConfiguracion.do?accion=goBsqAdmEmpleado  
Petición POST:  
txtDni=&txtApPaterno=ramirez&txtApMaterno=&txtNombres=
```

Figura 5: Solicitud URL enviada al servidor de aplicaciones

[Fuente: Informe Técnico Kunak Consulting].

Evidencia:

Se accede al sistema con un usuario que no tiene perfil ADMINISTRADOR.

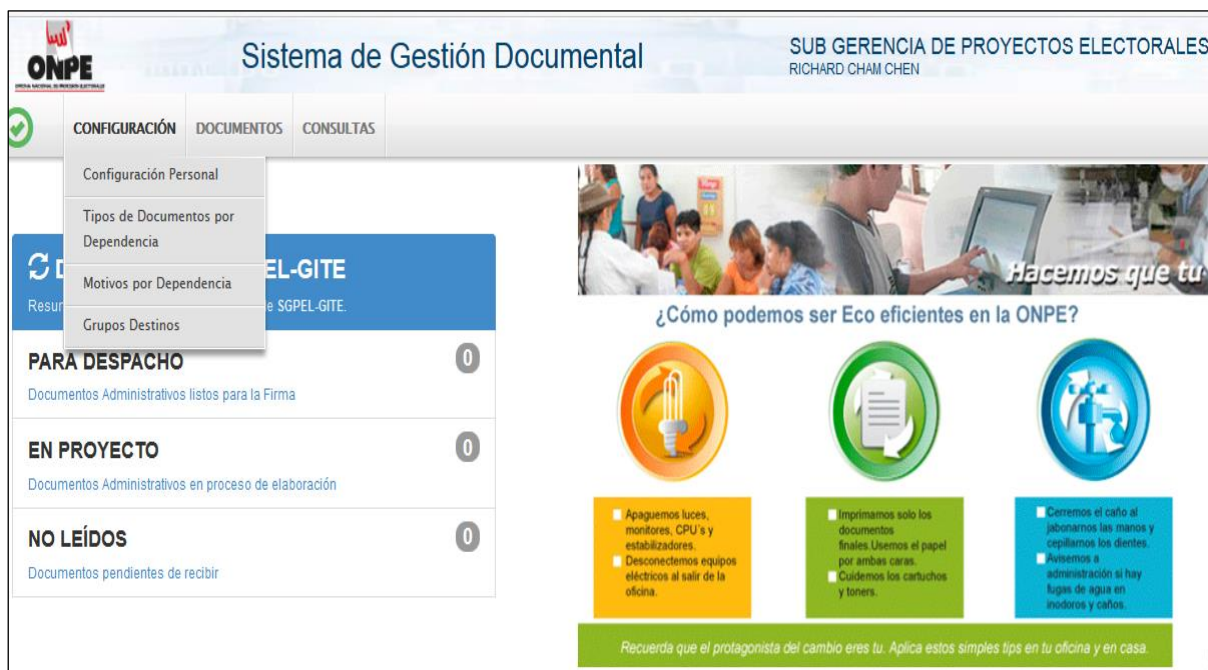


Figura 6: Usuario con perfil BÁSICO, no cuenta con las opciones de perfil ADMINISTRADOR en el módulo de CONFIGURACION

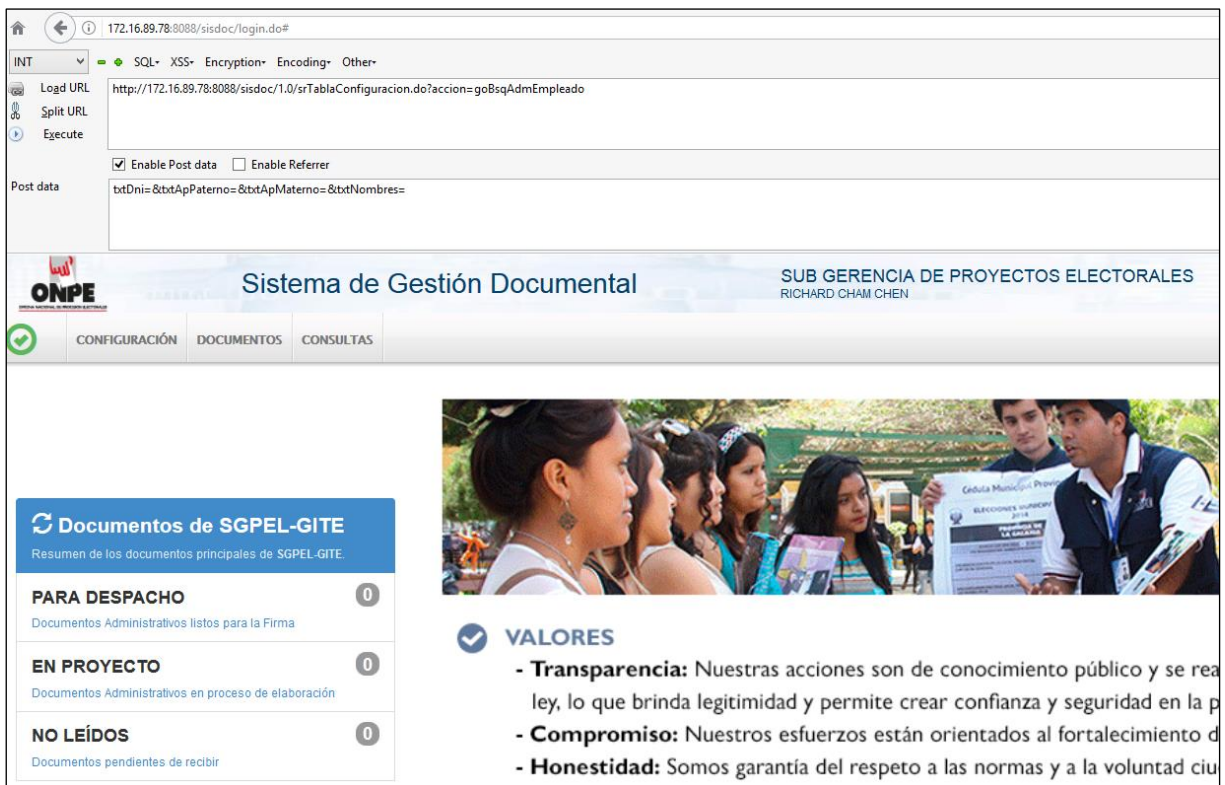


Figura 7: Evidencia de acceso no autorizado a las opciones de perfil ADMINISTRADOR.

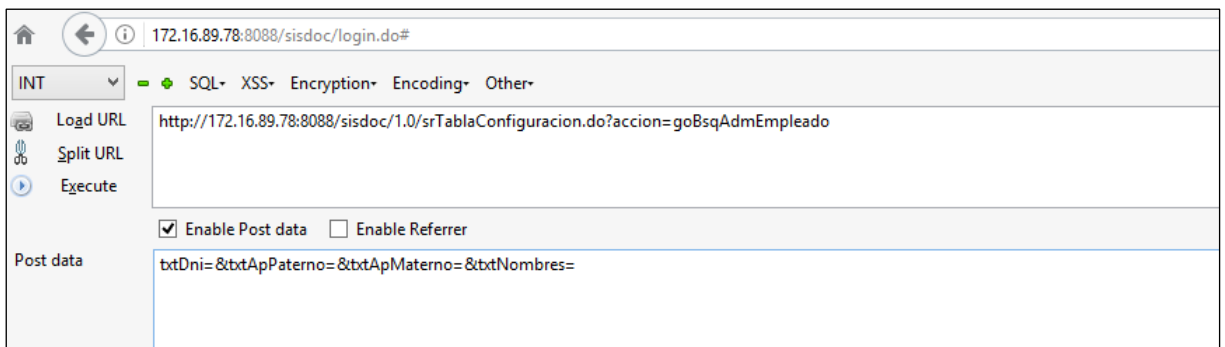


Figura 8: Envío de Request URL al servidor de aplicaciones, utilizando la herramienta HackBar.

INT SQL XSS Encryption Encoding Other					
Load URL Split URL Execute					
http://localhost:8088/sisdoc/1.0/srTablaConfiguracion.do?accion=goBsqAdmEmpleado					
Enable Post data Enable Referrer					
Post data					
txtDni=&txtApPaterno=&txtApMaterno=&txtNombres=					
Cod	DNI	Ap. Paterno	Ap. Materno	Nombres	
00442	07177876	BLAS	CERON	SANTOS VIRGILIO	
00443	48038412	BRAVO DE RUEDA	VEGA	CECILIA AIDA MILAGROS	
00444	41390923	BRAVO	CHEGNI	WILMER FELIX	
00445	41619923	BRIONES	CHENG	JORGE AUGUSTO	
00446	10147561	BRIONES	HERAS	MAURICIO	
00447	09963959	CABALLERO	FLORES	LUIS ABDON	
00448	10476790	CALDAS	PALACIOS	MANUEL IVAN	
00449	32989203	CALDERON DE LA BARCA	PORTILLO	MARCOS HUGO	
00450	42922271	CALIXTO	RUBIO	FELIX RAUL	
00451	46788646	CALLAMPI	CHUCHON	GIANINA ZULEIKA	
00452	29726368	CAMA	VALENCIA	JOSE LUIS	
00453	07007227	CAMAYO	SOLSOL	SARA NATIVIDAD	
00454	21116776	CAMPAÑA	VILCHEZ	SONIA RUTH	
00455	40133599	CAMPOS	APONTE	KARINA ELIZABETH	
00456	07543219	CAMPOS	VALDERRAMA	JAIME	
00457	16729987	CAMPOS	CHUMACERO	MARIELA ESTHER	
00458	46742683	CAMPOS	VERA	GONZALO SPENCER	
00459	16333371	CANALE	BEQUELM	DAVID ANTONIO	

Figura 9: Evidencia de acceso no autorizado a la opción buscar empleado, privilegio del perfil ADMINISTRADOR.

Finalmente, luego de realizar las validaciones correspondientes, al intentar vulnerar el sistema, donde se ingresa la misma Request URL ingresados en la evidencia, el sistema mostrará un mensaje indicando que el recurso solicitado no fue encontrado.



Figura 9: Vulnerabilidad controlada.

Estas validaciones fueron aplicadas a las siguientes opciones del Módulo de CONFIGURACION del sistema:

- ✓ Administración de Empleados.
- ✓ Registro de Requisitos.
- ✓ Administración de Perfiles.
- ✓ Registro de Proveedores.
- ✓ Registro TUPA.
- ✓ Tipos de Documento por Dependencia.
- ✓ Motivos por Dependencia.
- ✓ Grupos Destinos.
- ✓ Acceso a la Información a Dependencias Adicionales.
- ✓ Administración de UUOO.
- ✓ Administración de Funcionarios.
- ✓ Configuración Personal.

2. Validar y restringir el acceso al detalle de los documentos administrativos, personales y de Mesa de Partes a aquellos usuarios que intenten acceder y/o modificar información que no le corresponda.

Se implementó validaciones de acceso en la capa de control (Controller). De esta manera cuando un usuario intente acceder a una opción de los módulos Documentos, Mesa de Partes y Consultas y/o al detalle de un documento administrativo o personal y/o al modificar el estado de un documento, se realizará la comparación del código de empleado y el código de dependencia del usuario en sesión con el código de empleado que elabora y/o recibe el documento y el código de dependencia de este.

En la evaluación realizada sobre el Sistema de Gestión Documental por parte de Kunak Consulting, se identificó sobre varias funciones del sistema que estos enviaban diversos parámetros a través del método POST, pudiendo luego un eventual atacante modificar para

obtener acceso a secciones restringidas.

Pruebas sobre la sección DOCUMENTOS:

Para realizar las pruebas de Ethical Hacking se realizaron las siguientes operaciones sobre el sistema de información:

1. Se accede con el usuario RCHAM
2. Accede a la sección DOCUMENTOS
3. Se accede a la sección EMISION DE DOCUMENTOS y se obtiene el listado de documentos emitidos.
4. Se selecciona un documento del listado y se da clic en la opción EDITAR.

Se obtiene la siguiente petición:



Figura 10: Manipulación de parámetros en la opción Editar Documentos.

Allí se puede identificar el parámetro PNUEMI, el mismo que contiene un valor identificativo de la emisión.

5. Se ingresa con el usuario RCHAM.

6. Se coloca la petición identificada en el paso 04 y se accede a información no permitida.

Como resultado de las pruebas, es posible acceder al detalle de los documentos emitidos por otros usuarios del sistema de información sin contar con los privilegios para acceder a estos.

Evidencia:

The screenshot displays the 'Sistema de Gestión Documental' interface for the 'SUB GERENCIA DE PROYECTOS ELECTORALES' user 'RICHARD CHAM CHEN'. The interface includes a navigation bar with 'CONFIGURACIÓN', 'DOCUMENTOS', and 'CONSULTAS'. Below this, there's a section for 'EMISION DE DOCUMENTOS ADMINISTRATIVOS' with buttons for 'Nuevo', 'Editar', 'Ver Documento', 'Ver Anexos', 'Seguimiento', and 'Salir'. A 'Configuración Búsqueda' section contains input fields for 'Nro Emisión', 'Nro Documento', 'Expediente', and 'Asunto', along with a 'Buscar' button and a checkbox for 'Otros Resultados (?)'. A 'Configuración Filtro' section shows 'AÑO: 2018' and 'Prioridad: ..TODOS:'. Below these is a 'Detalle' table with columns: 'Nº', 'REFERENCIA ORIGEN', 'FECHA', 'TIPO DOC.', 'Nº DOCUMENTO', 'ASUNTO', and 'DESTINO'. The table currently shows 'No se encuentran registros.' At the bottom, there's a footer with 'Equipo: Trámite Documentario', 'Versión 1.0', 'Ruta de Documentos: C:\Users\jcalixto\Documents\TDOCUMENTOS', and 'Unidad Orgánica: SUB GERENCIA DE PROYECTOS ELECTORALES SEDE CENTRAL'.

Figura 11: Evidencia que el usuario RCHAM no tiene acceso al número de emisión 2600.

EMISION DE DOCUMENTOS ADMINISTRATIVOS

Expediente

Número: JAVC0020180000016 Fecha: 21/02/2018

Proceso:

Año: 2018 EN PROYECTO

Nro Emisión: 2600

Remitente

Dependencia: SUB GERENCIA DE PROYECTOS ELECTORALES

Firmado Por: GOMEZ AGUILA CHRISTIAN DAVID

Elaborado Por: HIJAR CONTRERAS MANUEL MARTIN

Documento

Tipo: INFORME Número: -2018 -SGPEL-GITE

ACTUALIZACIÓN DE APLICACIONES TECNOLÓGICAS PARA EL APOYO EN

Figura 12: Evidencia de acceso NO autorizado a información a través de la manipulación de parámetros por el usuario RCHAM.

Post data

http://localhost:8088/sisdoc/1.0/srDocumentoAdmEmision.do?accion=goEditDocumentoEmi

Figura 13: Evidencia de acceso no autorizado a información a través de la manipulación de parámetros por el usuario RCHAM.

Finalmente luego de implementar las validaciones correspondientes, al intentar vulnerar el sistema, donde se ingresa la misma Request URL ingresados en la evidencia, el sistema mostrará un mensaje indicando que el recurso solicitado no fue encontrado.

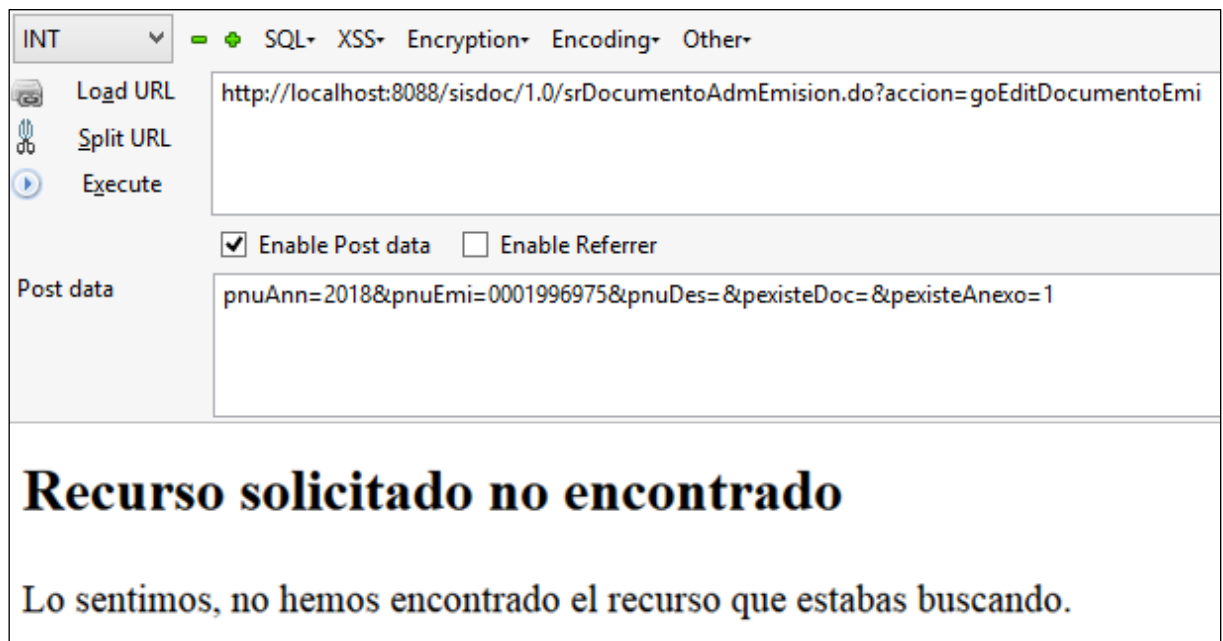


Figura 14: Vulnerabilidad controlada.

Estas validaciones fueron aplicadas a las siguientes funcionalidades del sistema:

- ✓ Editar Documento Administrativo.
- ✓ Editar Documento Personal.
- ✓ Editar Documentos Externos.
- ✓ Detalle Documentos Emitidos.
- ✓ Detalle Documentos Recibidos.
- ✓ Detalle Documentos Visto Bueno.
- ✓ Detalle Documentos Personales.
- ✓ Detalle Seguimiento de Emitidos.
- ✓ Detalle Seguimiento de Recibidos.
- ✓ Detalle Documentos Externos.
- ✓ Detalle Seguimiento Documentos Externos.
- ✓ Generar Documento.

3. Implementar la encriptación de parámetros enviados por URL al servidor de aplicaciones.

Se procedió a implementar la encriptación de parámetros, del lado del cliente, enviados al servidor de aplicaciones, para ello se modificó la lógica de programación. Se utilizó además una serie de técnicas de encriptación y librerías de JavaScript para dicho propósito. Del mismo modo se procedió a implementar filtros de servlets para el proceso de inicio de sesión de formulario así como técnicas desenscriptacion de parámetros de lado del servidor.

Cabe mencionar que la encriptación de parámetros aplica a todas las opciones de los módulos del sistema de Gestión Documental.

Inicialmente, en la evaluación realizada sobre el Sistema de Gestión Documental por parte de Kunak Consulting, se realizaron pruebas de Manipulación de Parámetros del sistema. Esta

prueba tenía por objetivo obtener acceso y/o modificar solicitudes (REQUEST) del sistema de información para acceder a secciones restringidas o realizar operaciones sobre el sistema de información. Se identificó que se enviaba diversos parámetros a través del método POST, pudiendo luego un eventual atacante modificar para obtener acceso a secciones restringidas.

Para realizar las pruebas de Ethical Hacking se realizaron las siguientes operaciones sobre el sistema de información:

1. Se accede con el usuario JCALIXTO.
2. Se Accede a cualquier sección del Sistema de Gestión Documental.
3. Se accede a cualquier opción del sistema.

Allí se puede identificar que los valores de los parámetros sTipoDeBusqueda, sCoDependencia, sFechaEmiIni, sFechaEmiFin etc. No están encriptados.

Evidencia:

SGPEL-Sistema de Gestión Docu

localhost:8088/sisdoc/login.do#



Sistema de Gestión Documental

SUB GERENCIA DE PROYECTOS ELECTORALES
JUAN CARLOS CALIXTO SALAZAR

CONFIGURACIÓN

DOCUMENTOS

MESA DE PARTES

CONSULTAS

Emisión de Documentos

Recepción de Documentos

Emisión Personal

Documentos

Resumen de los documentos

PARA DESPACHO 14

EN PROYECTO 57

MUY URGENTES 77

URGENTES 4

NO LEÍDOS 526

Rumbo a la excelencia

IMPLEMENTANDO LAS 5S

¿Qué son las 5 S?

5S es una herramienta de gestión que ayuda a mejorar el ambiente de trabajo volviéndolo un lugar más seguro, agradable y altamente productivo.

1
Seleccionar y eliminar los objetos innecesarios en el lugar de trabajo
SELECCIÓN

2
Un lugar para cada cosa y cada cosa con su etiqueta
ORDEN

3
Mantener el entorno de trabajo limpio y ordenado, eliminando las fuentes de suciedad
LIMPIEZA

4
Definir las normas que permitan mantener el nivel alcanzado
ESTANDARIZAR

5
Crear el hábito de las buenas prácticas y mejora continua
DISCIPLINA

Equipo: Trámite Documentario
Versión 1.0
Ruta de Documentos:

Unidad Orgánica:
SUB GERENCIA DE PROYECTOS ELECTORALES
SEDE CENTRAL

Figura 15: Evidencia de parámetros de envío sin encriptación en todas las opciones del sistema.



Sistema de Gestión Documental

SUB GERENCIA DE PROYECTOS ELECTORALES
JUAN CARLOS CALIXTO SALAZAR

CONFIGURACIÓN

DOCUMENTOS

MESA DE PARTES

CONSULTAS

EMISION DE DOCUMENTOS ADMINISTRATIVOS

Nuevo

Editar

Ver Documento

Ver Anexos

Seguimiento

Salir

Configuración Búsqueda

Nro Emisión:

Nro Documento:

Expediente:

Asunto:

Buscar

Otros Resultados (?)

Incluir Filtro

Configuración Filtro

AÑO: 2018

Prioridad: ..TODOS..

Detalle

N°	REFERENCIA ORIGEN	FECHA	TIPO DOC.	N° DOCUMENTO	ASUNTO	DESTINATARIO
2600	SUB GERENCIA DE PROYECTOS E	21/06/2018	INFORME	-2018-SGPTEL-GITE	ACTUALIZACIÓN DE APLICACIONES TECNOLÓGICAS PARA EL APOYO EN E	GERENCIA DE INFORMATICA Y TECNOL

Elements

Console

Sources

Network

Performance

Memory

Application

Security

Audits

View:

Group by frame

Preserve log

Disable cache

Offline

Online

Filter

Hide data URLs

XHR

JS

CSS

Img

Media

Font

Doc

WS

Manifest

Other

5 ms

10 ms

15 ms

20 ms

25 ms

30 ms

35 ms

40 ms

45 ms

50 ms

55 ms

60 ms

65 ms

70 ms

75 ms

80 ms

85 ms

90 ms

95 ms

Name

X

Headers

Preview

Response

Cookies

Timing

srDocumentoAdmEmision.do?accion=goInicio

Query String Parameters (1)

Form Data

view source

view URL encoded

sTipoBusqueda: 0

sCoDependencia: 2220

sCoEmpleado:

sTiAcceso:

esFiltroFecha: 2

sFeEmilni: 01/01/2018

sFeEmiFin: 31/12/2018

sBandejaEntrada: 1

sNumCorEmision:

sNumDoc:

sBuscNroExpediente:

sDeAsuM:

1 / 2 requests

54.3 KB / 54.3 KB transferred

Figura 16: Evidencia de parámetros de envío sin encriptación en todas las opciones del sistema.

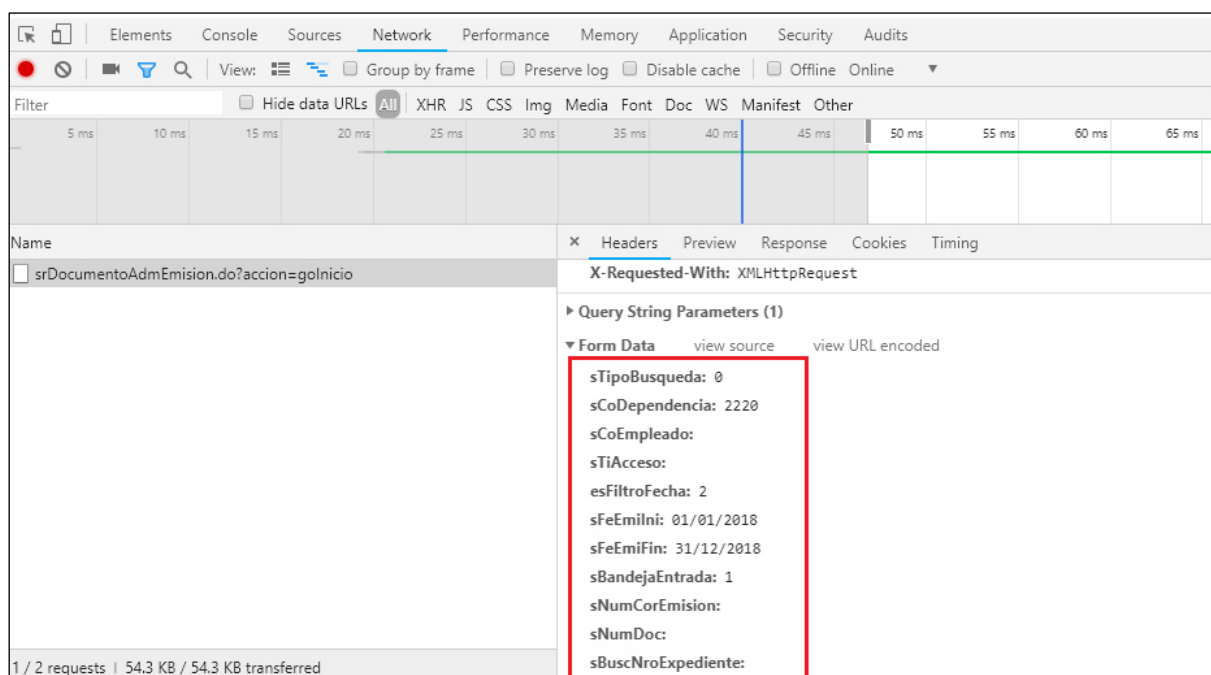


Figura 17: evidencia de parámetros de envío sin encriptación en todas las opciones del sistema.

Finalmente después de implementar la encriptación de parámetros, al intentar manipular los parámetros para utilizarlos en alguna solicitud URL, estos no contendrán los valores reales.

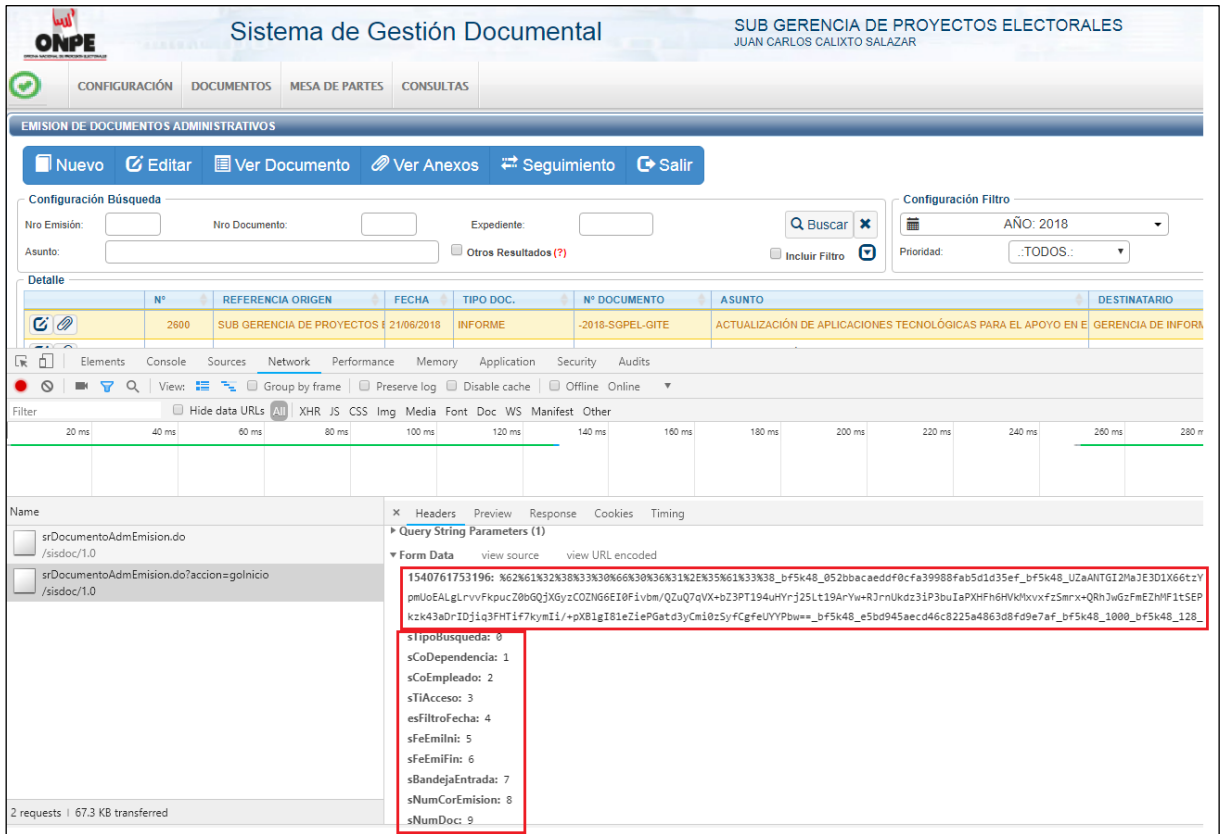


Figura 18: Parámetros de envío encriptado.

En la zona sombreada se aprecia la encriptación global en un solo parámetro, esto para reducir tiempos de respuesta por parte del servicio.

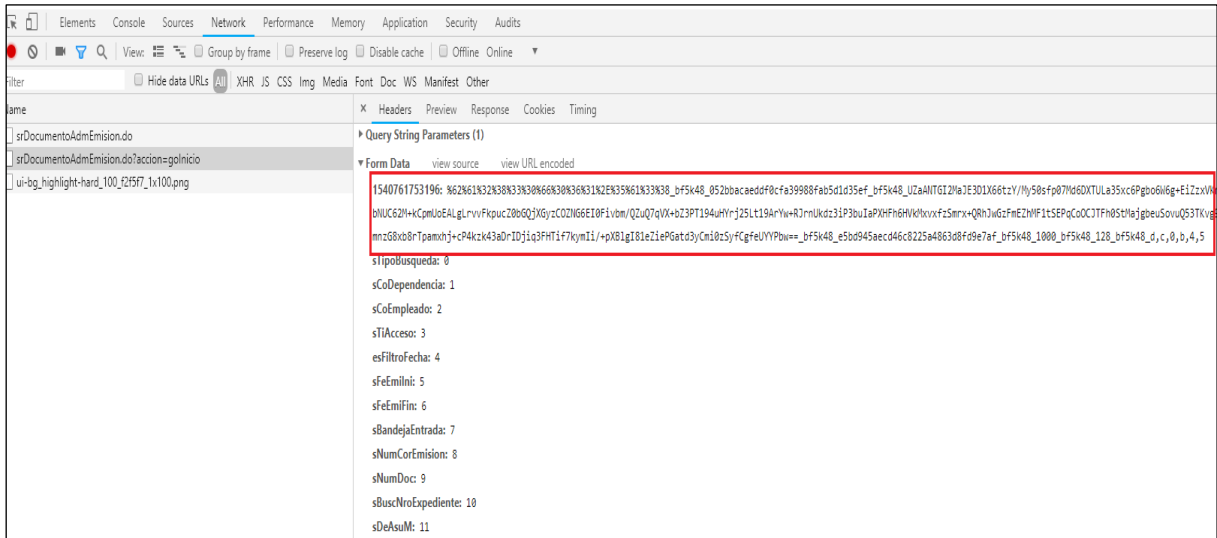


Figura 19: parámetros de envío encriptados.

En la región sombreada se muestra los parámetros enviados con sus respectivos valores alterados. Esto con el fin de despistar a un posible atacante.

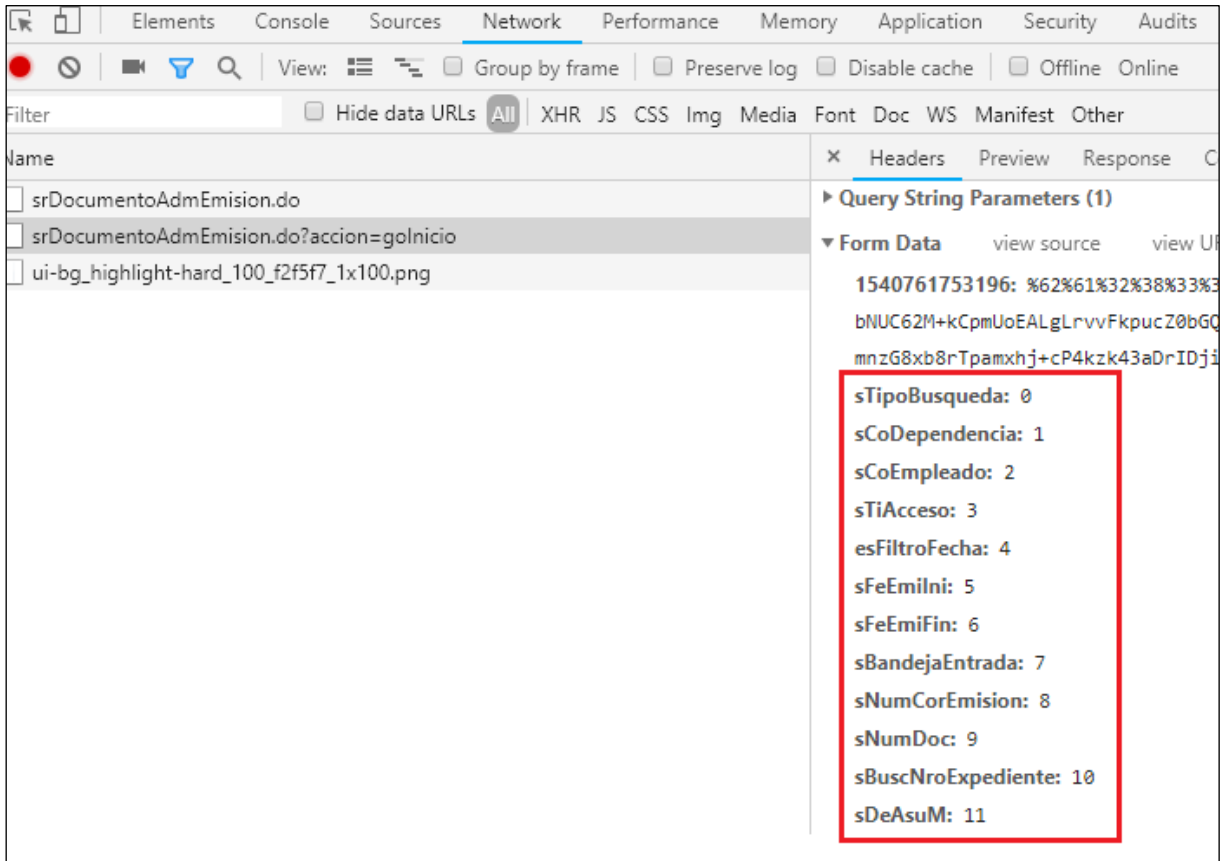


Figura 20: Parámetros de envío enumerados.

4. Realizar la actualización de la versión de la biblioteca multiplataforma jQuery.

Se procedió a realizar la actualización de la biblioteca multiplataforma jQuery a la versión 3.3.1, esto debido a que “*existían vulnerabilidades del tipo de secuencias de comandos entre sitios (Cross-site scripting o XSS)*” permitiendo ejecutar ataques de tipo “*Expresión regular de denegación de servicio (ReDoS)*” que es un ataque algorítmico de complejidad que produce una denegación de servicio, Ataque Distribuido de denegación de Servicios (DDoS) , DOM Based Cross-site Scripting” de carácter medio y “XSS in dialog closeText” de carácter alto, todo lo anteriormente mencionado permite al atacante engañar al navegador de un usuario para ejecutar código JavaScript malicioso en el contexto del dominio, tales scripts pueden robar las cookies de sesión del usuario para el dominio, modificar su contenido, y realizar o modificar acciones en nombre del usuario. Estaban involucradas las librerías jQuery1.10.1, jQuery UI 1.10.3 y Moment.js 2.4.0 que se encontraban en el Sistema de Gestión Documental.

Evidencia:



Figura 21: Ejecución de la herramienta Audits del navegador Chrome.



Sistema de Gestión Documental

SUB GERENCIA DE PROYECTOS ELECTORALES

JUAN CARLOS CALIXTO SALAZAR

CONFIGURACIÓN

DOCUMENTOS

MESA DE PARTES

CONSULTAS

Documentos de SGPEL-GITE

Resumen de los documentos principales de SGPEL-GITE.

PARA DESPACHO

Documentos Administrativos listos para la Firma

25

EN PROYECTO

82

Elements

Console

Sources

Network

Performance

Memory

Application

Security

Audits

127.0.0.1 - localhost:8080

Best Practices

73

1 Does not use HTTP/2 for all of its resources

62 requests not served via HTTP/2

2 Page is missing the HTML doctype

Expected systemid to be an empty string

Specifying a doctype prevents the browser from switching to quirks-mode. Read more on the [MDN Web Docs page](#)

3 Includes front-end JavaScript libraries with known security vulnerabilities

5 vulnerabilities detected

Some third-party scripts may contain known security vulnerabilities that are easily identified and exploited by attackers.

Learn more

Library Version	Vulnerability Count	Highest Severity
jQuery@1.10.1	1	Medium
jQuery UI@1.10.3	1	High
Moment.js@2.4.0	3	Medium

4 Uses deprecated APIs

1 warning found

Passed audits

11 audits

Runtime settings

Figura 22: Resultados de la ejecución de la herramienta Audits del navegador Chrome.

Finalmente después de actualizar jQuery a la versión 3.3.1, la observación realizada por la herramienta es subsanada.

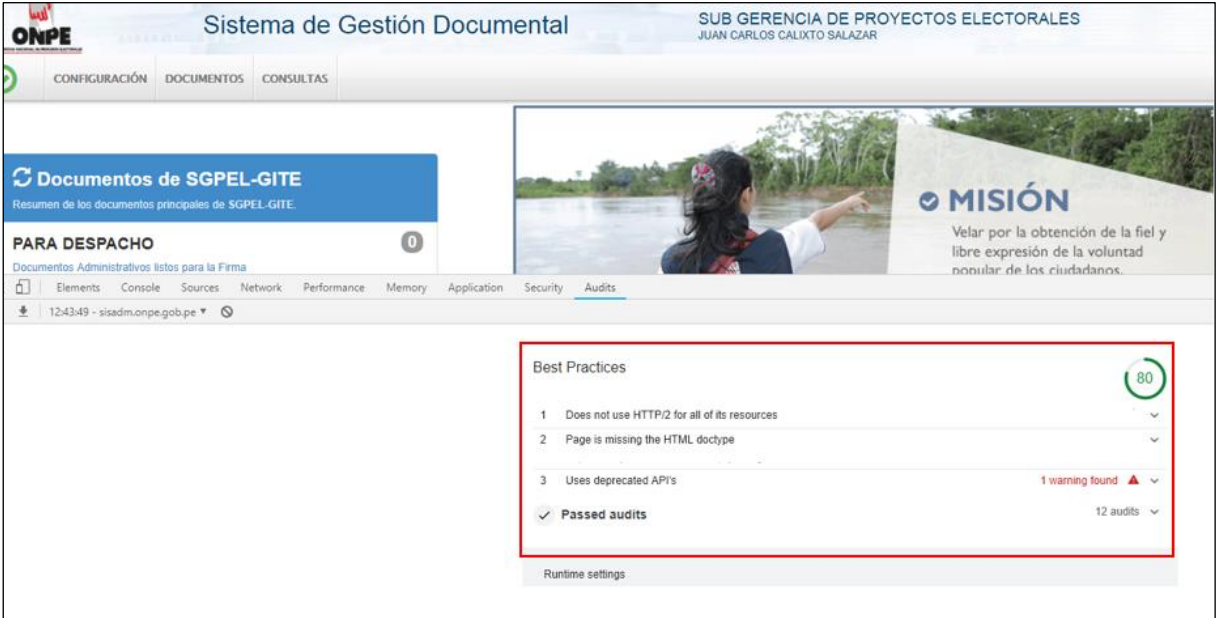


Figura 23: Observación subsanada al realizar la actualización del jQuery.

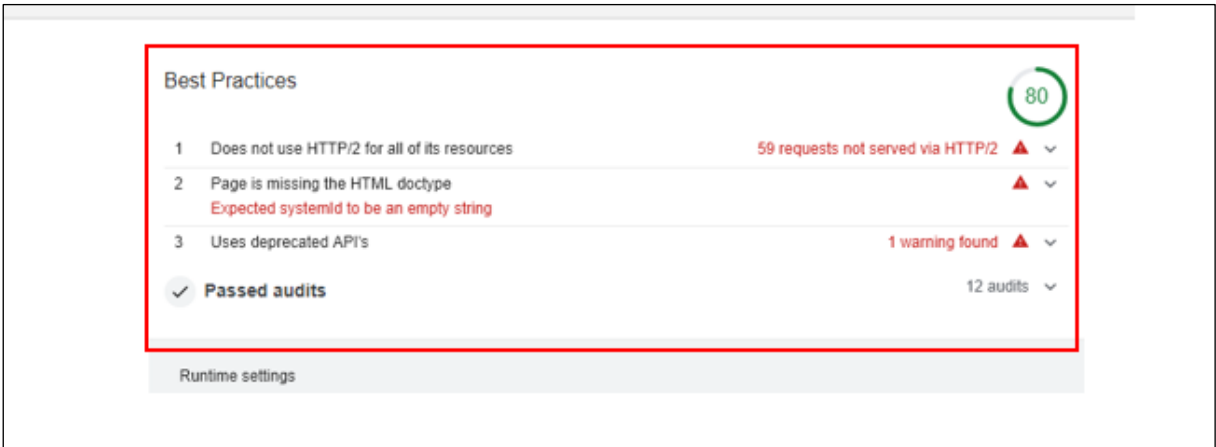


Figura 24: Imagen Ampliada Observación subsanada al realizar la actualización del jQuery.

5. Implementar librería propia de imagen Captcha.

Se implementó una librería de imagen Captcha de desarrollo propio, para el inicio de sesión al Sistema de Gestión Documental y evitar así ataques de acceso recurrente. Esta implementación cumple los siguientes requisitos:

- a. La imagen captcha aparece al tercer intento de acceso al sistema.
- b. El usuario será bloqueado al quinto intento de ingresar el código captcha y la contraseña correspondiente.
- c. La imagen captcha cuenta con las siguientes características técnicas para dificultar su obtención mediante programas OCR:
 - Caracteres alfanuméricos (letras + números).
 - Caracteres con grados de inclinación.



ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES

Sistema de Gestión Documental

Usuario

Contraseña

[Ingresar](#)

El usuario o la contraseña es incorrecta.

[Requisitos del sistema](#) [Manual de usuario](#) [Cambiar contraseña](#)

Figura 25: Usuario accediendo al sistema.



Figura 26: Imagen Captcha Luego de ingresar erróneamente la contraseña.



Figura 27: Usuario es bloqueado luego de ingresar erróneamente la contraseña y el Captcha.

Cabe resaltar que el número máximo de intentos de error al ingresar la contraseña sin el captcha y con el captcha respectivamente, son configurables desde el archivo **application.properties**, esto quiere decir que la persona encargada de configurar el sistema, podrá definir el valor de dichos parámetros.

6. Realizar cambio a nivel de lógica de programación del sistema sobre el formulario de acceso al sistema.

Se realizó el cambio a nivel de lógica de programación del sistema sobre el formulario de acceso al sistema. A continuación se muestra el nuevo flujo del proceso de autenticación:

- a. Ingreso de usuario de acceso al sistema.
- b. Ingreso de contraseña de acceso al sistema.
- c. Botón de acceso al sistema.

En caso las credenciales sean correctas:

Procesar la Dependencia a la cual pertenece y otorgar los permisos requeridos.

En caso las credenciales sean incorrectas:

Mostrar un mensaje indicando: “Usuario y/o contraseña incorrecta”.

Inicialmente durante las revisiones y análisis de vulnerabilidades sobre el formulario de acceso al Sistema de Gestión Documental por parte de Kunak Consulting, se identificó que el formulario permitía realizar la enumeración de usuarios que se encontraban registrados en el sistema. Como resultado de las pruebas, se identificó lo siguiente:

Si se coloca un usuario que existe se obtiene: la dependencia a la que pertenece. Si se coloca un usuario que NO EXISTE se obtiene: “usuario no tiene acceso al sistema”. En base al proceso de enumeración fue posible identificar muchos usuarios del sistema de información.

Riesgo de Seguridad:

1. Un eventual atacante identifica los usuarios del sistema de información a través de revisiones manuales.
2. Con los usuarios identificados en el paso 01, el atacante realiza un ataque de fuerza bruta sobre el usuario hasta lograr ingresar al sistema de información.

Evidencia:



Sistema de Gestión Documental

Usuario

Contraseña

Dependencia 

 Ingresar

Usuario no tiene acceso al sistema.

 Requisitos del sistema  Manual de usuario

Figura 28: Evidencia enumeración de cuentas de usuarios en el sistema.



ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES

Sistema de Gestión Documental



Usuario ERAMIREZC

Contraseña

Dependencia JEFATURA DE AREA DE ATENCION A
↻

Ingresar

[Requisitos del sistema](#)
[Manual de usuario](#)

Figura 29: Evidencia enumeración de cuentas de usuarios en el sistema.

Nro.	Usuario	Código Empleado	Código Departamento	Nombre de Departamento	Número de Intento	Número de intentos realizados	Número de intento máximo
1		'coEmp':	'coDep':	'deDep':JEFATURA DE AREA DE ARCHIVO ELECTORAL Y VERIFICACION DE FIRMAS	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
2		'coEmp':	'coDep':	'deDep':SUB GERENCIA DE FINANZAS	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
3		'coEmp':	'coDep':	'deDep':SUB GERENCIA DE ASESORIA ADMINISTRATIVA	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
4		'coEmp':	'coDep':	'deDep':OFICINA REGIONAL DE COORDINACION PUCALLPA	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
5		'coEmp':	'coDep':	'deDep':JEFATURA DE AREA DE NORMATIVA Y REGULACION DE FINANZAS PARTIDARIAS	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
6		'coEmp':	'coDep':	'deDep':SUB GERENCIA DE RECURSOS HUMANOS	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
7		'coEmp':	'coDep':	'deDep':SUB GERENCIA DE RELACIONES CORPORATIVAS	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
8		'coEmp':	'coDep':	'deDep':GERENCIA DE GESTION ELECTORAL	'nuint':1'	'nuintMax':3'	'nuintMaxCapt':5'
9		'coEmp':	'coDep':	'deDep':JEFATURA NACIONAL	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
10		'coEmp':	'coDep':	'deDep':OFICINA REGIONAL DE COORDINACION ICA	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
11		'coEmp':	'coDep':	'deDep':SUB GERENCIA DE OPERACIONES INFORMATICAS	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
12		'coEmp':	'coDep':	'deDep':JEFATURA DE AREA DE ARCHIVO ELECTORAL Y VERIFICACION DE FIRMAS	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
13		'coEmp':	'coDep':	'deDep':JEFATURA DE AREA DE PLATAFORMA TECNOLOGICA	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
14		'coEmp':	'coDep':	'deDep':JEFATURA DE AREA DE PLATAFORMA TECNOLOGICA	'nuint':1'	'nuintMax':3'	'nuintMaxCapt':5'
15		'coEmp':	'coDep':	'deDep':JEFATURA DE AREA DE VERIFICACION Y CONTROL	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
16		'coEmp':	'coDep':	'deDep':OFICINA REGIONAL DE COORDINACION CAJAMARCA	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
17		'coEmp':	'coDep':	'deDep':SUB GERENCIA DE COMUNICACIONES Y PRENSA	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
18		'coEmp':	'coDep':	'deDep':SUB GERENCIA DE FORMACION Y CAPACITACION ELECTORAL	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
19		'coEmp':	'coDep':	'deDep':PROCURADURIA PUBLICA	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
20		'coEmp':	'coDep':	'deDep':SUB GERENCIA DE RELACIONES CORPORATIVAS	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
21		'coEmp':	'coDep':	'deDep':OFICINA REGIONAL DE COORDINACION TRUJILLO	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
22		'coEmp':	'coDep':	'deDep':GERENCIA DE GESTION ELECTORAL	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
23		'coEmp':	'coDep':	'deDep':PROCURADURIA PUBLICA	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
24		'coEmp':	'coDep':	'deDep':SUB GERENCIA DE ASISTENCIA TECNICA	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'
25		'coEmp':	'coDep':	'deDep':SUB GERENCIA DE ORGANIZACION ELECTORAL DESCONCENTRADA	'nuint':0'	'nuintMax':3'	'nuintMaxCapt':5'

Figura 30: El atacante obtiene lista de empleados.

Finalmente luego de seguir las recomendaciones por parte de Kunak Consulting se procedió a modificar la lógica de programación del sistema sobre el formulario de acceso al sistema.



Figura 31: Evidencia enumeración de cuentas de usuarios en el sistema.



Figura 32: Vulnerabilidad Controlada.

7. Modificar a nivel de programación la estructura de las respuestas de cabeceras de todas las páginas que componen al Sistema de Gestión Documental.

Se procedió a implementar una serie de cabeceras en los filtros de servlets para el proceso de inicio de sesión de formulario:

- X-Frame-Options: se utiliza para evitar que la web pueda ser vulnerada en un frame, o iframe. Así se pueden evitar ataques de clickjacking sobre la página.
- X-Content-Type-Options: al enviar esta cabecera en la respuesta con el valor “nosniff”, los navegadores que soportan esta cabecera (IE y Chrome), no cargan las hojas de estilos, ni los scripts (JavaScript), cuyo Myme-type no sea el adecuado.
- X-XSS-Protection: Este encabezado se usa para configurar la protección contra un XSS reflejado.
- Strict-Transport-Security: permite decirle a un navegador que siempre quiere que un usuario se conecte usando HTTPS en lugar de HTTP. Esto significa que cualquier marcador, enlace o dirección forzará a los usuarios a usar HTTPS, incluso si especifican HTTP.

En la fase VII: Implantación

En esta fase se realizaron pruebas internas por parte del equipo de desarrollo, se utilizaron las mismas herramientas que utilizó Kunak Consulting para realizar el servicio de Ethical Hacking. Seguido de esto se realizó el pase al área de control de calidad, finalmente se obtuvo el informe de conformidad para el respectivo pase a producción.

3.4 EVALUACIÓN ECONÓMICA:

Todas las actividades llevadas a lo largo del presente trabajo fueron desarrolladas en la Oficina Nacional de Procesos Electorales, con cargo al presupuesto anual y a sus planes operativos, por tratarse de una institución del estado no fue necesario realizar un análisis costo beneficio que implique incrementos presupuestales provenientes erario fiscal, pero como referencia se indica el gasto realizado de este proyecto.

- ✓ Costo del Proyecto.
- ✓ Personal requerido por mes.
- ✓ Flujo de pagos.

Duración del Proyecto: 5 meses

Fecha de Inicio: 23/04/2018 al 28/08/2018

Flujos de Pago	Abril 2018 (S/.)	Mayo 2018 (S/.)	Junio 2018 (S/.)	Julio 2018 (S/.)	Agosto 2018 (S/.)	Total
Líder de Proyecto	8,000.00	8,000.00	8,000.00	8,000.00	8,000.00	40,000.00
Analista de Sistemas	3,500.00	3,500.00	3,500.00	3,500.00	3,500.00	17,500.00
Programador 1	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	25,000.00
Programador Web	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	22,500.00
PCs Core I7	16,000.00	0.00	0.00	0.00	0.00	16,000.00
Impresora Laser	2,500.00	0.00	0.00	0.00	0.00	2,500.00
Servidor File Server	8,000.00	0.00	0.00	0.00	0.00	8,000.00
Windows 8 Profesional	16,000.00	0.00	0.00	0.00	0.00	16,000.00
MS office 2013	2,500.00	0.00	0.00	0.00	0.00	2,500.00
Java	0.00	0.00	0.00	0.00	0.00	0.00
Oracle	8,000.00	0.00	0.00	0.00	0.00	8,000.00
Teléfono	200.00	200.00	200.00	200.00	200.00	1,000.00
Luz	250.00	250.00	250.00	250.00	250.00	1,250.00
Agua	120.00	120.00	120.00	120.00	120.00	600.00
Suministro de Computo	200.00	200.00	200.00	200.00	200.00	1,000.00
COSTO TOTAL	74,770.00	21,770.00	21,770.00	21,770.00	21,770.00	161,850.00

Tabla 2: Flujo de caja del proyecto

CAPITULO IV. REFLEXION CRITICA DE LA EXPERIENCIA

4.1 APORTES EN EL AREA DE DESARROLLO Y RESPONSABILIDADES

La colaboración en el informe fue con el rol de analista programador para realizar la implementación de buenas prácticas en seguridad informática al sistema de gestión documental en los módulos: Configuración, Documentos, Mesa de Partes, Consultas.

La participación principal del suscrito fue la de implementar validaciones de accesos por roles y privilegios a las diferentes opciones que cuentan los usuarios del Sistema de Gestión Documental, además de validar y restringir el acceso al detalle de los documentos administrativos, personales y de Mesa de Partes a aquellos usuarios que intenten acceder y/o modificar información que no le corresponda.

Participación en la actualización del documento Especificación de Requerimientos del Software (ERS-415) cuyo fin es brindar una guía fácil y de rápido entendimiento para las áreas usuarias, describiendo las funciones a ser implementadas en el Mantenimiento al Sistema de Gestión Documental.

Participación en la actualización del documento Reglas de Negocio (RN-415) cuyo objetivo es identificar y especificar detalladamente las reglas del negocio definidas en el desarrollo del Mantenimiento del Sistema de Gestión Documental.

Como todo sistema, el desarrollo logrado puede ser mejorado y actualizado teniendo en cuenta el permanente desarrollo de las tecnologías de la información y en particular de las herramientas de desarrollo.

CAPITULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Se realizó las validaciones accesos por roles y privilegios a las diferentes opciones que cuentan los usuarios del Sistema de Gestión Documental.
- Se evitó la manipulación de parámetros mediante la transferencia de información a través de la encriptación de parámetros en el envío de las peticiones.
- Se implementó la librería de imagen Captcha para evitar ataques de acceso recurrente.
- Se modificó la lógica de programación de acceso al Sistema de Gestión Documental para evitar transferencia de información innecesaria.
- Se modificó a nivel de programación la estructura de las respuestas de cabeceras de todas las páginas que componen el sistema.

5.2 RECOMENDACIONES

- La ONPE debe ampliar y mantener políticas de seguridad con altos estándares actualizadas de acuerdo al avance tecnológico. Por ejemplo, las contraseñas son el mecanismo de autenticación más utilizado actualmente por lo que es importante definir políticas específicas para establecer contraseñas.
- Se debe realizar periódicamente capacitaciones sobre seguridad informática a todos los empleados de la ONPE para reducir el riesgo de ser atacados. Es importante informar sobre ataques de ingeniería social, ya que es una de las metodologías más utilizadas por los atacantes.
- Es recomendable que la ONPE realice análisis de sus vulnerabilidades de forma periódica para corregir problemas de seguridad, no solo en el caso del Sistema de Gestión Documental sino en la generalidad de sistemas elaborados para los Procesos Electorales.
- Es recomendable incluir personal capacitado en servicios de Ethical Hacking al área de Aseguramiento de la Calidad.

FUENTES DE INFORMACIÓN

NTP ISO/IEC 12207. (06 de 10 de 2011). NTP ISO/IEC 12207. Obtenido de NTP ISO/IEC 12207: <http://ctn-issi.pucp.pe/normas-tecnicas-peruanas/ntp-iso-iec-12207>

IEEE 24774-2012. (29 de 03 de 2012). IEEE 24774-2012. Obtenido de IEEE 24774-2012: <https://standards.ieee.org/standard/24774-2012.html>

kunak. (2017). informe técnico. lima: kunak consulting ciber security. Obtenido de informe técnico.

NTP ISO/IEC 15504. (11 de 04 de 2012). NTP ISO/IEC 15504. Obtenido de NTP ISO/IEC 15504: <http://ctn-issi.pucp.pe/normas-tecnicas-peruanas/ntp-iso-iec-15504>

ONPE. (01 de 01 de 2007). portal onpe. Obtenido de portal onpe: <https://www.onpe.gob.pe>

GLOSARIO

- **ARCHIVO:**
Conjunto de documentos conservados por cualquier técnica en cualquier medio actualmente conocido o recientemente desarrollado.
- **ÁREA DE CALIDAD DE SOFTWARE:**
Área de la organización encargada de validar los requisitos y requerimientos de un producto de software antes de aprobar su pase a producción.
- **DOCUMENTO**
Medio que tenga en él información registrada y que pueda ser tratado como una unidad
- **FRAMEWORK:**
Entorno de trabajo que facilita el desarrollo de aplicaciones en cualquier lenguaje de programación.
- **ETHICAL HACKING:**
Es el proceso por el cual, se utilizan las mismas técnicas y herramientas que un black hat para atacar a una organización y descubrir las vulnerabilidades de la misma.
- **RUP:**
El Proceso Unificado Racional o RUP (por sus siglas en inglés de Rational Unified Process) es un proceso de desarrollo de software desarrollado por la empresa Rational Software, actualmente propiedad de IBM.¹

- **FIRMA DIGITAL:**
 Datos adjuntos de una unidad de datos que permite al receptor de la unidad de datos comprobar el origen y la integridad de la unidad de datos y proteger contra falsificación, por ejemplo, por el receptor.

- **HTML:**
 Lenguaje de programación que se utiliza para el desarrollo de páginas de internet.

- **JAVA SERVER PAGE (JSP):**
 Componente visual que interactúa directamente con el usuario, utiliza lenguaje java y HTML.

- **MANUAL DE USUARIO:**
 Documento que describe la funcionalidad del sistema y como puede ser utilizado por los diferentes usuarios según sus perfiles.

- **NORMA TÉCNICA PERUANA:**
 Conjunto de buenas prácticas basadas en normas e isos internacionales que regulan una serie de procesos y procedimientos dentro del país.

- **GLASSFISH:**
 Es un servidor de aplicaciones que utiliza tecnología J2EE y a la vez es un servidor web.

- **ONPE:**
 Organismo público y autónomo encargado es la autoridad máxima en la organización y ejecución de los procesos electorales de referéndum y otros.

- **SPRING:**
 Es un framework o entorno de trabajo utilizado facilitar el desarrollo de aplicaciones multicapas, utilizando tecnología java.

- AUDITS:

Es una herramienta automatizada de código abierto diseñada para mejorar la calidad de las apps web. Se puede ejecutar como una extensión de Chrome o desde la línea de comandos.

ANEXOS

Tabla de contenido

ANEXO 1- INFORME TÉCNICO.....	71
Introducción	72
Credenciales Brindadas	73
Resumen Ejecutivo de Vulnerabilidades Identificadas en el Sistema de Gestión Documental	74
Metodología de Cuantificación de las Vulnerabilidades	75
Listado de Vulnerabilidades Identificadas en el Sistema de Gestión Documental.....	76
Inadecuada Gestión de Privilegios: Acceso No Autorizado a las opciones del perfil Administrador	77
Inadecuada Gestión de Privilegios: Acceso No Autorizado al detalle de los documentos emitidos/recepcionados por usuarios sección CONSULTAS	83
Inadecuada Gestión de Privilegios: Acceso No Autorizado al detalle de los documentos emitidos/recepcionados por usuarios sección DOCUMENTOS.....	88
Inadecuada Gestión de Privilegios: Acceso No Autorizado al detalle de los documentos recepcionados por usuarios sección MESA DE PARTES	92
Inadecuada Gestión de Privilegios: Recepción de documentos de manera no autorizada	97
Inadecuada Gestión de Privilegios: Carga/modificación de documentos de manera no autorizada	101
Formulario de acceso al sistema susceptible a ataques recurrentes de acceso.....	104
Formulario de acceso permite la enumeración de usuarios del sistema de información	107
Identificación de información innecesaria transferida en las solicitudes enviadas en el sistema de información	111
Debilidades en las cabeceras del protocolo HTTP	114

ANEXO 2 – PASE A CONTROL DE CALIDAD	116
Solicitud de Creación de Carpeta.....	116
Confirmación de Ruta de Carpeta Creada	117
Formato de Solicitud de Pase a Control de Calidad	118
Informe de Conformidad de Control de Calidad	122
ANEXO 3 – PASE A PRODUCCIÓN.....	123
Solicitud de Pase a Producción	123
Formato de Solicitud de Pase de Producción	124

ANEXOS 1 : INFORME TECNICO.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 1 de 76



CYBER SECURITY

ETHICAL HACKING – SGD – CONVENIOS – FUNC2017



INFORME TÉCNICO

Documento en versión final

Introducción

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS –	Código: EH-ONPE -IT
	FUNC 2017	Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 4 de 76

Introducción

Kunak Consulting ha llevado a cabo un servicio de escaneo de vulnerabilidades y test de penetración sobre el sistema de información SGD (Sistema de Gestión Documental) de la OFICINA NACIONAL DE PROCESOS ELECTORALES (ONPE). Mediante este servicio se pretende determinar el nivel de riesgo de seguridad que poseen los elementos tecnológicos de la institución desde una perspectiva EXTERNA.

Las pruebas se realizaron desde la siguiente perspectiva (escenarios):

1. **BLACKBOX** (caja negra): la perspectiva de un usuario normal, es decir, sin privilegios y sin conocer nombres de usuarios o contraseñas.
2. **GRAYBOX** (caja gris): la perspectiva de un usuario con acceso al sistema, es decir, se brindaron credenciales de acceso para las pruebas al sistema.

Sobre ambos escenarios se incluye la revisión de un marco de los principales componentes tecnológicos de la institución, entendiendo estos como servidores y equipos de comunicaciones y dispositivos de seguridad.

La identificación de vulnerabilidades incluye la revisión de configuraciones en relación a las buenas prácticas de programación, falta de actualización del software utilizado, uso de configuraciones por defecto, configuraciones débiles o erróneas, entre otras vulnerabilidades técnicas.

Adicionalmente las pruebas son un medio para verificar la efectividad de las políticas y controles de seguridad de la información que existen actualmente en la institución.

Finalmente se generan recomendaciones a partir de los resultados obtenidos para corregir los problemas encontrados.

1. Alcance

Las pruebas de vulnerabilidad se realizaron a la siguiente aplicación web desde una perspectiva externa e interna respectivamente:

1.1. Sistemas de Información:

Nro.	Sistema de Información	Dirección URL
1	Aplicación principal	https://sisadm.onpe.gob.pe
2	Aplicación Notificador	https://sisadm.onpe.gob.pe/notificador/
3	Aplicación Web Socket	https://sisadm.onpe.gob.pe/sgdwserver/

1.2. Ethical Hacking Externo:

Nro.	Dirección IP Pública
1	200.37.33.199

Credenciales brindadas por la ONPE para las pruebas respectivas de Ethical Hacking

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 5 de 76

1.3. Credenciales brindadas:

Para la realización de pruebas en CAJA GRIS el equipo de la Oficina Nacional de Procesos Electorales (ONPE) proporcionó al equipo consultor de KUNAK CONSULTING las siguientes credenciales de acceso:

Nro.	Perfil	Usuario	Contraseña
1	Administrador	ERAMIREZC	
2	Mesa de partes	DBARRIOS	
3	Básico	NESPIRITU	

Resumen Ejecutivo de Vulnerabilidades Identificadas.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017		Código: EH-ONPE -IT
			Versión: 3.0
			Fecha: 03/10/17
	Informe Técnico – Primer Escaneo		Página: 6 de 76

2. Resumen Ejecutivo de Vulnerabilidades Identificadas

Calificación de las Vulnerabilidades

Leyenda de los riesgos identificados

Categoría	Alto	Medio	Bajo
Nivel de riesgo			

Vulnerabilidad Alta: en esta clasificación se encuentran las vulnerabilidades que son ampliamente explotadas, que tienen herramientas de explotación conocidas y ampliamente difundidas y en algunos casos estas no requieren de un gran conocimiento para su uso, incluyendo también virus, gusanos o troyanos. Constituyen un compromiso total del sistema o una segura negación de servicio. Se incluyen aquí instalaciones por defecto con usuarios de altos privilegios con contraseñas débiles o sin ellas.

Vulnerabilidad Media: Aquí entran todas aquellas vulnerabilidades que no comprometen la integridad del sistema directamente o que no se conocen herramientas que puedan explotar aún estas vulnerabilidades. Constituyen un paso medio en el proceso de ataque. Permiten fugas de información para ataques más elaborados o defectos menores de sistema o de implementación que afectan el rendimiento o uso normal del sistema sin causar una negación de servicio.

Vulnerabilidad Baja: En esta categoría se encuentran las vulnerabilidades que apenas pueden considerarse como peligrosas. Constituyen pequeñas fugas de información de sistema, comportamientos que permiten mapeo de la red o simplemente saber si el sistema se encuentra activo. Se consideran vulnerabilidades porque con el tiempo si no son atendidas sirven como medio para ataques más elaborados. No se conocen herramientas especiales para su explotación, simplemente su funcionamiento normal genera estos pequeños defectos.

Metodología de Cuantificación de las Vulnerabilidades

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 7 de 76

Metodología de cuantificación de las Vulnerabilidades (CVSS)

La metodología utilizada por Kunak Consulting para la valoración del riesgo de seguridad de información de las vulnerabilidades identificadas como parte del servicio de Ethical Hacking se encuentra soportada en el estándar CVSS (Common Vulnerability Scoring System) y la experiencia de nuestros consultores.

El CVSS es una iniciativa pública concebida por la National Infrastructure Assurance Council (NIAC) de EE.UU, un grupo que provee de recomendaciones al Department of Homeland Security de los EE.UU. Entre las organizaciones que lo adoptaron tempranamente destacan Cisco, US National Institute of Standards and Technology (NIST), Qualys y Oracle. En la actualidad, el CVSS está bajo la custodia del Forum for International Response Teams (FIRST) y es aceptada por diversas organizaciones relacionadas a seguridad de información: IBM, HP, CISCO, MICROSOFT, McAfee, Symantec, etc.

Entre los beneficios que ofrece el CVSS están:

1. **Puntuación estándar de vulnerabilidades:** El CVSS es neutro desde el punto de vista de las aplicaciones, permitiendo que distintas organizaciones asignen una puntuación a sus vulnerabilidades de TI a través de un único esquema.
2. **Puntuación contextualizada:** La puntuación asignada por una institución corresponde al riesgo que la vulnerabilidad representa para dicha institución.
3. **Sistema abierto:** El CVSS provee todos los detalles sobre los parámetros usados en la generación de cada puntuación permitiendo comprender tanto el razonamiento que sustenta una puntuación como el significado de diferencias entre puntuaciones.

Las puntuaciones asignadas por el CVSS se derivan de los tres grupos de métricas siguientes:

- **Base:** Este grupo representa las propiedades de una vulnerabilidad que son inmutables en el tiempo, específicamente: complejidad de acceso, vector de acceso, y grado en que compromete la confidencialidad, integridad y disponibilidad del sistema.
- **Temporal:** Este grupo mide las propiedades de una vulnerabilidad que sí cambian en el tiempo, como por ejemplo la existencia de parches o código para su explotación.
- **Entorno:** Este grupo mide las propiedades de una vulnerabilidad que son representativas de los ambientes de uso de las TI como por ejemplo la prevalencia de sistemas afectados y pérdidas potenciales.

Para mayor detalle del mecanismo utilizado para la valoración del riesgo asociado a CVSS, recomendamos visitar la siguiente página web: <http://www.first.org/cvss>



Listado de Vulnerabilidades Identificadas en el Sistema de Gestión documental

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 8 de 76

Vulnerabilidades Identificadas:

Vulnerabilidades Identificadas según su criticidad			
Nro.	Descripción de la vulnerabilidad identificada y el riesgo asociado	Categoría	CVSS
Vulnerabilidades – Sistema de Gestión Documental (SGD)			
1	Inadecuada Gestión de Privilegios: Acceso NO autorizado a las opciones del perfil ADMINISTRADOR Se identificó que usuarios que no cuentan acceso al perfil Administrador pueden acceder a opciones de dicha sección		8.5
2	Inadecuada Gestión de Privilegios: Acceso NO autorizado al detalle de documentos emitidos/recepcionados por usuarios (sección CONSULTAS) Se identificó que usuarios que no cuentan con permisos para listar y observar el detalle de documentos emitidos pueden acceder a estos a través de la manipulación de parámetros.		7.5
3	Inadecuada Gestión de Privilegios: Acceso NO autorizado al detalle de documentos emitidos/recepcionados por usuarios (sección DOCUMENTOS) Se identificó que usuarios que no cuentan con permisos para listar y observar el detalle de documentos emitidos pueden acceder a estos a través de la manipulación de parámetros.		7.5
4	Inadecuada Gestión de Privilegios: Acceso NO autorizado al detalle de documentos recepcionados por usuarios (sección MESA DE PARTES) Se identificó que usuarios que no cuentan con permisos para listar y observar el detalle de documentos recepcionados pueden acceder a estos a través de la manipulación de parámetros.		7.5
5	Inadecuada Gestión de Privilegios: Recepción de documentos de manera NO autorizada Se identificó que usuarios que no cuentan con permisos para recepcionar documentos pueden hacerlo suplantando la identidad de otros usuarios.		7.5
6	Inadecuada Gestión de Privilegios: Carga/modificación de documentos de manera NO autorizada. Se identificó que a través de la modificación de parámetros es posible cargar y/o modificar documentos asociados a documentos emitidos.		7.5
7	Formulario de acceso al sistema susceptible a ataques recurrentes de acceso Se identificó que el formulario de acceso cuentan con controles débiles que prevengan ataques recurrentes de acceso NO autorizado.		4.3
8	Formulario de acceso permite la enumeración de usuarios del sistema de información Se identificó que el formulario de acceso al sistema de información permite obtener o identificar si un usuario se encuentra registrado en el mismo.		4.3
9	Identificación de información innecesaria transferida en las solicitudes enviadas en el sistema de información. Se identificó que la solicitud de acceso al sistema transfiere información innecesaria que puede ser utilizada por un eventual atacante para realizar ataques.		4.3
10	Debilidades en las cabeceras del protocolo HTTP Se identificó que las cabeceras del protocolo HTTP no cuentan con controles para prevenir ataques del tipo XSS y además expone información innecesaria.		1.2

Inadecuada Gestión de Privilegios: Acceso no autorizado a las opciones del perfil ADMINISTRADOR

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 9 de 76

3. Detalle de las Vulnerabilidades Identificadas

A continuación, se presentan los resultados obtenidos durante las pruebas de seguridad realizadas sobre los sistemas de información e infraestructura tecnológica.

Vulnerabilidades en el Sistema de Gestión Documental (SGD)

3.1. Inadecuada Gestión de Privilegios: Acceso NO autorizado a las opciones del perfil ADMINISTRADOR

Descripción:

Durante el proceso de evaluación e identificación de vulnerabilidades, se realizaron pruebas de acceso NO autorizado a secciones restringidas que son PRIVILEGIADAS debido a la criticidad de las opciones que representan para el sistema de información. De manera puntual se realizaron pruebas de acceso a las opciones del perfil ADMINISTRADOR con usuarios que no cuentan con dicho privilegio.

El proceso de identificación de vulnerabilidades consiste en los siguientes pasos:

1. Se ingresa con el usuario ERAMIREZ, este usuario tiene el perfil: Administrador.
2. El usuario ERAMIREZ cuenta con la opción CONFIGURACIÓN en el MENU de opción principal.
3. La opción CONFIGURACIÓN cuenta con opciones designadas solo al perfil Administrador y que no pueden ser accedidas/ejecutadas por perfiles que no cuenten con dicho perfil.

Para probar la vulnerabilidad se realiza lo siguiente:

4. Se ingresa con el usuario NESPIRITU este usuario tiene el perfil: Básico
5. Este usuario no cuenta con privilegios a la opción CONFIGURACIÓN.
6. Sin embargo, si el usuario NESPIRITU ejecuta directamente los enlaces asociados al perfil Administrador las páginas pueden ser accedidas/ejecutadas debido a que no se valida los accesos a las páginas.

Para el ejemplo el usuario NESPIRITU accedió a la siguiente dirección URL:

```
https://sisadm.onpe.gob.pe/sgd/1.0/srTablaConfiguracion.do?accion=goBsqaAdmEmpleado
Petición POST:
txtDni=&txtApPaterno=ramirez&txtApMaterno=&txtNombres=
```

En el ejemplo mostrado un eventual atacante podría administrar usuarios, como, por ejemplo, habilitar o deshabilitar los mismos.

Como resultado de las pruebas se obtuvo que es posible que un usuario SIN PRIVILEGIOS pueda acceder a secciones reservadas para un usuario con el perfil de ADMINISTRADOR. Las secciones a que un usuario sin privilegio puede acceder son las siguientes:

Inadecuada Gestión de Privilegios: Acceso no autorizado a las opciones del perfil ADMINISTRADOR.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE-IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 11 de 76

Riesgo de Seguridad de Información

A continuación, se detallan los riesgos de seguridad de información asociados a la vulnerabilidad identificada:

1. Acceso NO autorizado a la administración de empleados
2. Acceso NO autorizado a la administración de perfiles
3. Acceso NO autorizado a la administración de UUOO.
4. En general acceso a las opciones del perfil ADMINISTRADOR.

Evidencia:

Evidencia

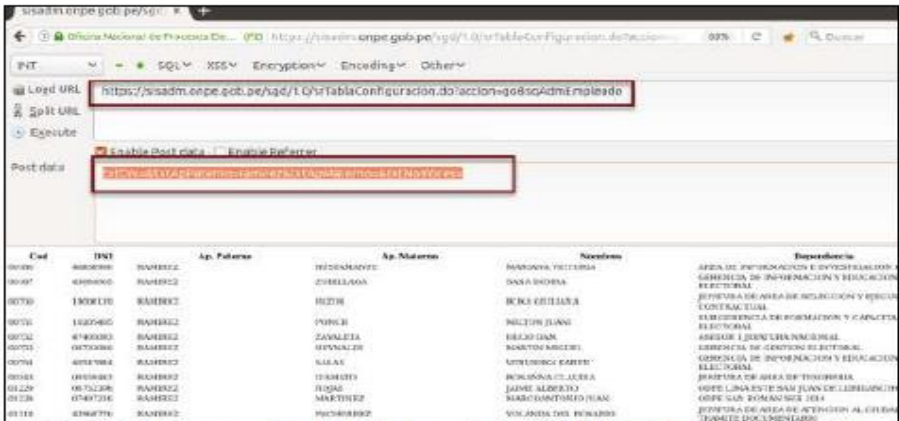


Fig1. Evidencia de acceso NO autorizado a la sección de ADMINISTRACIÓN y CONFIGURACIÓN

Inadecuada Gestión de Privilegios: Acceso no autorizado a las opciones del perfil ADMINISTRADOR.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE-IT
		Versión: 3.0
		Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 12 de 78

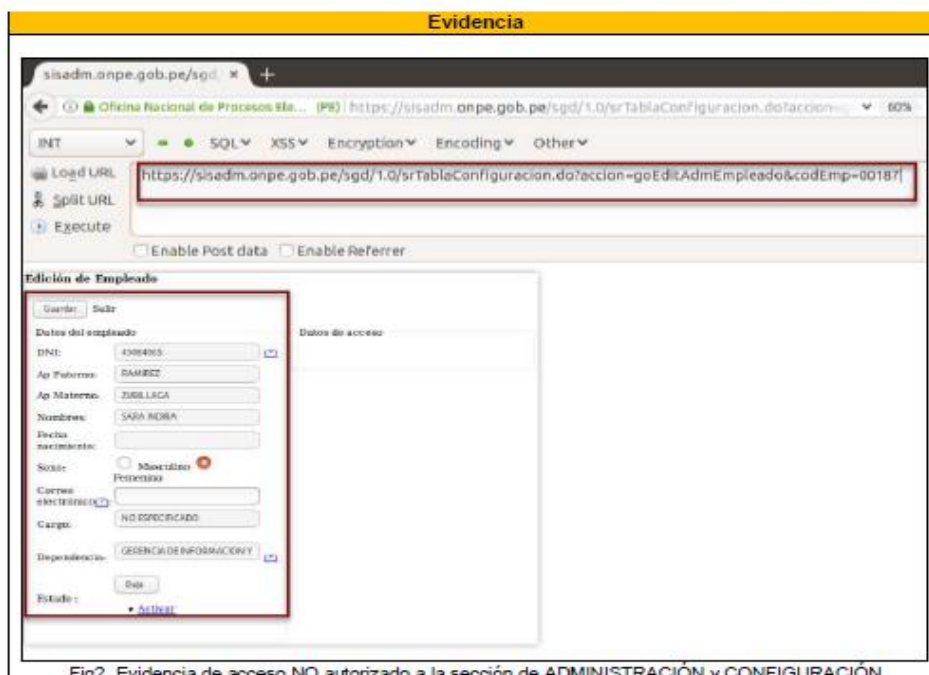


Fig2. Evidencia de acceso NO autorizado a la sección de ADMINISTRACIÓN y CONFIGURACIÓN

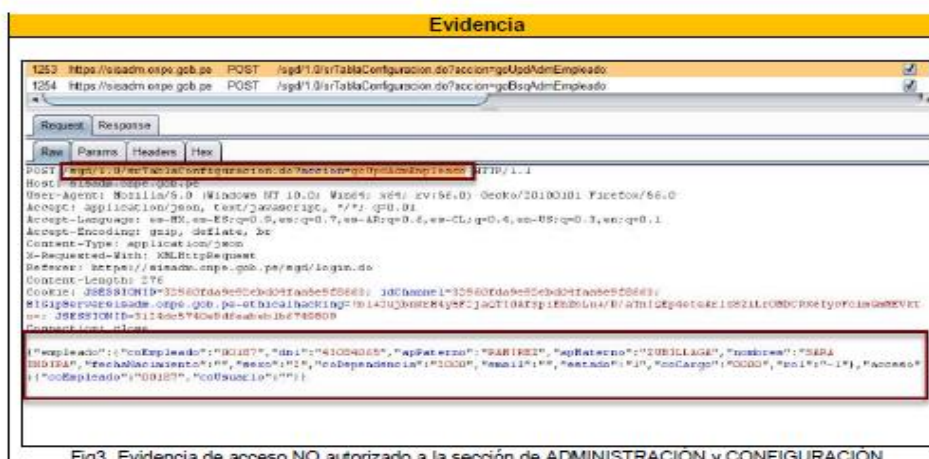
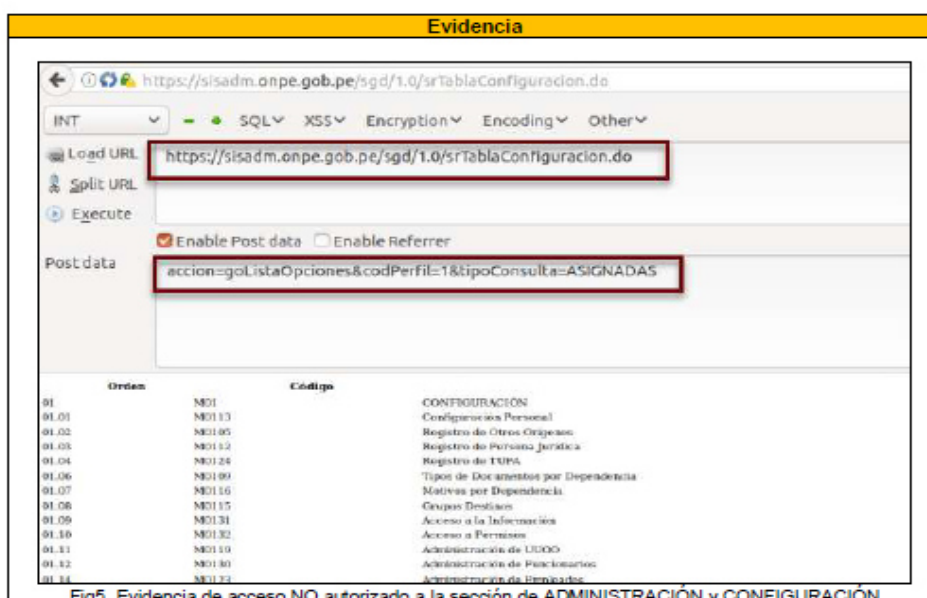
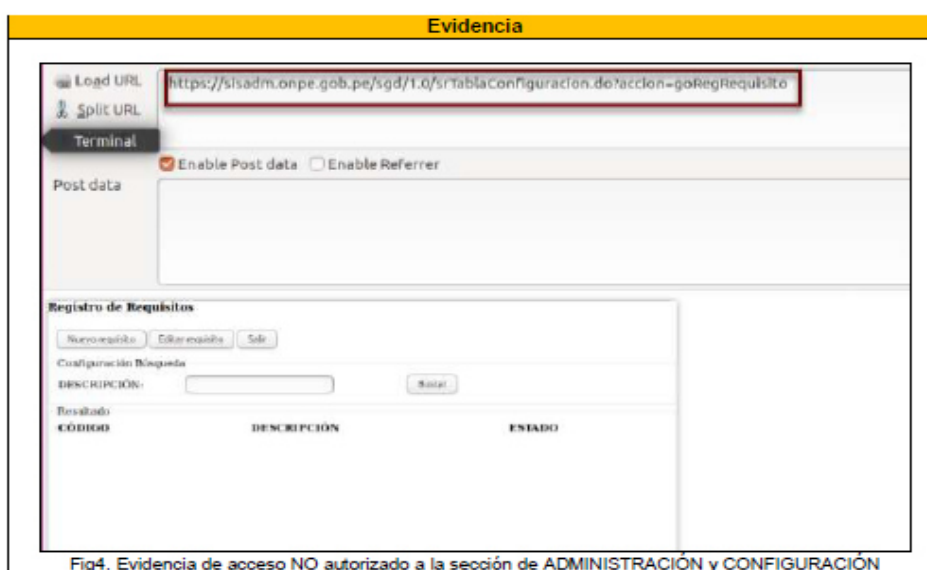


Fig3. Evidencia de acceso NO autorizado a la sección de ADMINISTRACIÓN y CONFIGURACIÓN

Inadecuada Gestión de Privilegios: Acceso no autorizado a las opciones del perfil ADMINISTRADOR.

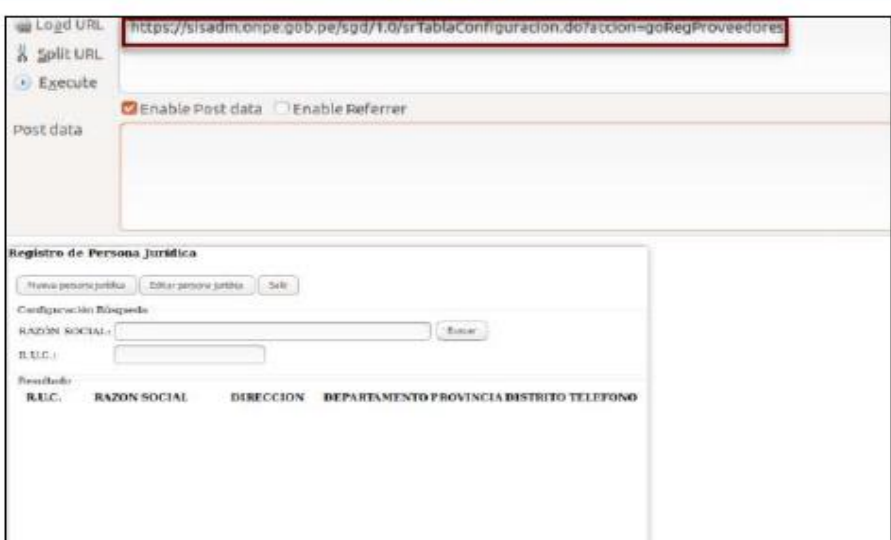
	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT Versión: 3.0 Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 13 de 76



**Inadecuada Gestión de Privilegios: Acceso no autorizado a las opciones del perfil
ADMINISTRADOR.**

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
	Informe Técnico – Primer Escaneo	Versión: 3.0
		Fecha: 03/10/17
		Página: 14 de 78

Evidencia



The screenshot shows a web application interface. At the top, a yellow banner reads 'Evidencia'. Below it, a browser window displays a URL: `https://sisadm.onpe.gob.pe/sgd/1.0/srTablaConfiguracion.do?accion=goRegProveedores`. The interface includes a sidebar with options like 'Load URL', 'Split URL', and 'Execute'. The main content area shows a search form for 'Registro de Persona Jurídica' with fields for 'RAZÓN SOCIAL' and 'R.U.C.', and a table header for search results.

Fig8. Evidencia de acceso NO autorizado a la sección de ADMINISTRACIÓN y CONFIGURACIÓN

Sistema Vulnerable:

Nro.	Sistema de Información	Proceso Vulnerable
1	Sistema de Gestión Documental	Sección CONFIGURACIÓN

Valoración de riesgo de la vulnerabilidad.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
	Informe Técnico – Primer Escaneo	Versión: 3.0
		Fecha: 03/10/17
		Página: 16 de 76

Valoración del Riesgo:

A continuación, se muestran los resultados de la valoración del riesgo de seguridad de información basada en el estándar CVSS (Common Vulnerability Scoring System):

Métricas de Puntuación Base	
Métricas de Explotabilidad	
Vector de Acceso	Remoto
Complejidad de Acceso	Medio
Autenticación requerida	Única
Métricas de Impacto	
Impacto en la confidencialidad	Completo
Impacto en la integridad	Completo
Impacto en la disponibilidad	Completo
Métricas de Puntuación Temporal	
Acceso a exploit	No definido
Corrección de vulnerabilidad disponible	No definido
Nivel de confiabilidad de la existencia de vulnerabilidad	No definido
Métricas de Puntuación del Entorno	
Potencial peligro colateral	No definido
Porcentaje distribuido de sistemas vulnerables	No definido

Resultados	
Puntuación Base CVSS	8.5
Subpuntuación de Impacto	10
Subpuntuación de Explotabilidad	6.8
Puntuación Temporal CVSS	No definido
Puntuación del Entorno CVSS	No definido
Puntuación Promedio CVSS	8.5

Inadecuada Gestión de Privilegios: Acceso no autorizado al detalle de los documentos emitidos/recepcionados sección CONSULTAS.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 17 de 76

3.2. Inadecuada Gestión de Privilegios: Acceso NO autorizado al detalle de los documentos emitidos/recepcionados por usuarios (sección CONSULTAS)

Descripción:

Durante el proceso de evaluación e identificación de vulnerabilidades, se realizaron pruebas de MANIPULACIÓN DE PARÁMETROS del sistema de información. La manipulación de parámetros tiene por objetivo obtener acceso y/o modificar solicitudes (REQUEST) del sistema de información para acceder a secciones restringidas o realizar operaciones sobre el sistema de información.

En la evaluación realizada sobre el sistema de información de la organización, se identificó que este envía diversos parámetros a través del método POST, pudiendo luego un eventual atacante modificar para obtener acceso a secciones restringidas.

Pruebas sobre la sección CONSULTAS:

Para realizar las pruebas se realizaron las siguientes operaciones sobre el sistema de información:

1. Se ingresó con el usuario ERAMIREZC y se realiza la emisión de un documento personal.
2. Luego se accede a la sección consultas "Documentos personales" y se identifica la URL asociada al documento emitido:



3. Se ingresa con otro usuario: NESPIRITU, este usuario no cuenta con registros de documentos personales emitidos.
4. Se colocan los parámetros identificados en el paso 02 y se accede a información reservada al usuario ERAMIREZC. Se identificó que a través de la modificación del parámetro PNUEMI se puede acceder a los archivos emitidos de otros usuarios. La técnica utilizada es la de FUZZING.

Como resultado de las pruebas, es posible acceder al detalle de los documentos personales y/o administrativos asociados a un usuario CON OTRO USUARIO que no cuenta con dichos privilegios.

Evidencia:

Inadecuada Gestión de Privilegios: Acceso no autorizado al detalle de los documentos emitidos/recepcionados sección CONSULTAS.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE-IT
		Versión: 3.0
		Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 18 de 78

Evidencia



Fig7. Evidencia de que el usuario NESPIRITU no tiene información asociada en la sección CONSULTAS

Evidencia

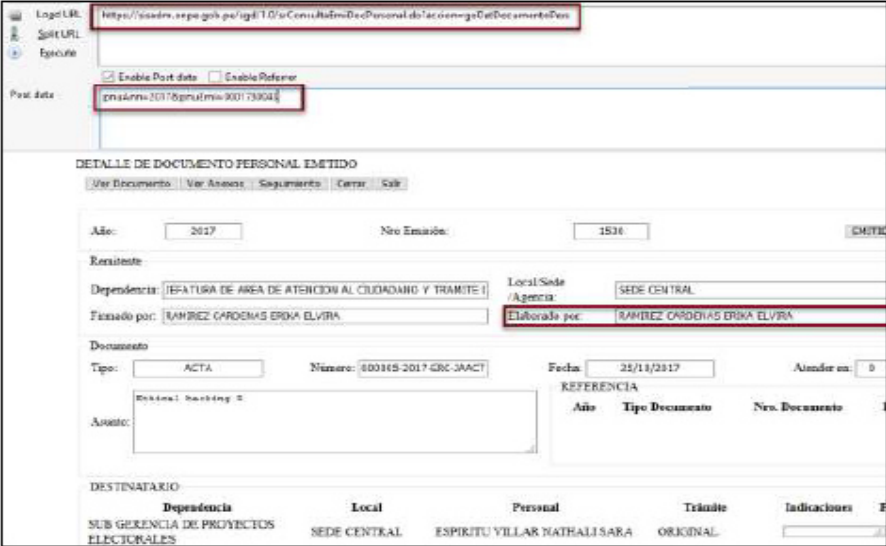


Fig8. Evidencia de acceso NO autorizado a información a través de la manipulación de parámetros

Inadecuada Gestión de Privilegios: Acceso no autorizado al detalle de los documentos emitidos/recepcionados sección CONSULTAS.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
		Fecha: 03/10/17
Informe Técnico – Primer Escaneo		Página: 19 de 76

Evidencia

https://sisadm.onpe.gob.pe/sgd/1.0/srConsultaEmiDocPersonal.do?accion=goDetDocumentoPers

☒ Enable Post data ☐ Enable Referrer

pnuAnn=2017&pnuEmi=000173004

DETALLE DE DOCUMENTO PERSONAL EMITIDO

Ver Documento Ver Anexos Seguir Seguimiento Cerrar Salir

Año: 2017 Nro Emisión: 1527

Remitente:

Dependencia: DEFATURA DE AREA DE ATENCION AL CIUDADANO Y TRAMITE I Local Sede /Agencia: SEDE CENTRAL

Firmado por: RAMIREZ CARDENAS ERIKA ELVIRA Elaborado por: RAMIREZ CARDENAS ERIKA ELVIRA

Documento:

Tipo: ACTA Número: 000002-2017-ERC-JA/ACT Fecha: 25/10/2017 Atender

SERVICIO DE ETHICAL HACKING 2

REFERENCIA

Año	Tipo Documento	Nro. Document

Asunto:

Fig9. Evidencia de acceso NO autorizado a información a través de la manipulación de parámetros

Evidencia

Request

Raw Params Headers Hex

```

POST /sgd/1.0/srConsultaEmiDocPersonal.do?accion=goDetDocumentoPers HTTP/1.1
Host: sisadm.onpe.gob.pe
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/plain, */*; q=0.01
Accept-Language: es-ES,es;q=0.9,es;q=0.7,es-AR;q=0.6,es-CL;q=0.4,en-US;q=0.3,en;q=0.1
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://sisadm.onpe.gob.pe/sgd/login.do
Content-Length: 29
Cookie: JSESSIONID=4250772668a84ba5ceaa17690db2; idChannel=4250772668a84ba5ceaa17690db2; BIGipServersisadm.onpe.gob.pe-ethicalhacking=xcs7Q3ByxOVWV9pIjaQTI0aI3pIERT/59 N8d2WCaJJcRD/E3onoX63rMajj8W1e7HAuL7tcR7bXcV9k=; JSESSIONID=3114dc5740e9d1eabed1be749809
Connection: close

pnuAnn=2017&pnuEmi=000173004

```

Fig10. Evidencia de acceso NO autorizado a información a través de la manipulación de parámetros

Inadecuada Gestión de Privilegios: Acceso no autorizado al detalle de los documentos emitidos/recepcionados sección CONSULTAS.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 20 de 76

Evidencia

Results
Target
Positions
Payloads
Options

Filter: Showing all items

Request	Payload	Status	Error	Redr...	Timeout	Length	Comment
31	40	200	☐	0	☐	6806	
30	39	200	☐	0	☐	6802	
32	41	200	☐	0	☐	6794	
33	42	200	☐	0	☐	6794	
34	43	200	☐	0	☐	6794	
0		404	☐	0	☐	531	
1	10	404	☐	0	☐	531	
2	11	404	☐	0	☐	531	
3	12	404	☐	0	☐	531	
4	13	404	☐	0	☐	531	
5	14	404	☐	0	☐	531	

Request
Response

Raw
Params
Headers
Hex

```

POST /sgd/1.0/srConsultaEmiDocPersonal.do?accion=gobecDocumentoPers HTTP/1.1
Host: sisadm.onpe.gob.pe
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-ES,en-US;q=0.9,en;q=0.7,en-AR;q=0.6,en-GB;q=0.4,en-US;q=0.3,en;q=0.1
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Cookie: 1dChannel=54e84c7af517ed17029eb060fc0; JSESSIONID=54e84c7af517ed17029eb060fc0;
810ip8server=sisadm.onpe.gob.pe-ethicalhacking=Ysc0tW1P0LZ12Hh3jauT10AF3p1KH5e/0nJRVyVtW+3p
subZbPc:Wp0CER25ldYF8k5q=F; JSESSIONID=5124deb740e9dewabab2b6749809
Connection: close
Upgrade-Insecure-Requests: 1
        
```

Fig11. Evidencia de acceso NO autorizado a información a través de la manipulación de parámetros de manera automatizada a través de técnicas de fuzzing

Sistema Vulnerable:

Nro.	Sistema de Información	Proceso Vulnerable
1	Sistema de Gestión Documental	Sección CONSULTAS

Valoración del Riesgo de la Vulnerabilidad.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
		Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 22 de 76

Valoración del Riesgo:

A continuación, se muestran los resultados de la valoración del riesgo de seguridad de información basada en el estándar CVSS (Common Vulnerability Scoring System):

Métricas de Puntuación Base	
Métricas de Explotabilidad	
Vector de Acceso	Remoto
Complejidad de Acceso	Medio
Autenticación requerida	Única
Métricas de Impacto	
Impacto en la confidencialidad	Completo
Impacto en la integridad	Parcial
Impacto en la disponibilidad	Parcial
Métricas de Puntuación Temporal	
Acceso a exploit	No definido
Corrección de vulnerabilidad disponible	No definido
Nivel de confiabilidad de la existencia de vulnerabilidad	No definido
Métricas de Puntuación del Entorno	
Potencial peligro colateral	No definido
Porcentaje distribuido de sistemas vulnerables	No definido
Resultados	
Puntuación Base CVSS	7.5
Subpuntuación de Impacto	8.5
Subpuntuación de Explotabilidad	6.8
Puntuación Temporal CVSS	No definido
Puntuación del Entorno CVSS	No definido
Puntuación Promedio CVSS	7.5

Inadecuada Gestión de Privilegios: Acceso no autorizado al detalle de los documentos emitidos/recepcionados sección DOCUMENTOS.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 23 de 76

3.3. Inadecuada Gestión de Privilegios: Acceso NO autorizado al detalle de documentos emitidos/recepcionados por usuarios (sección DOCUMENTOS)

Descripción:

Durante el proceso de evaluación e identificación de vulnerabilidades, se realizaron pruebas de MANIPULACIÓN DE PARÁMETROS del sistema de información. La manipulación de parámetros tiene por objetivo obtener acceso y/o modificar solicitudes (REQUEST) del sistema de información para acceder a secciones restringidas o realizar operaciones sobre el sistema de información.

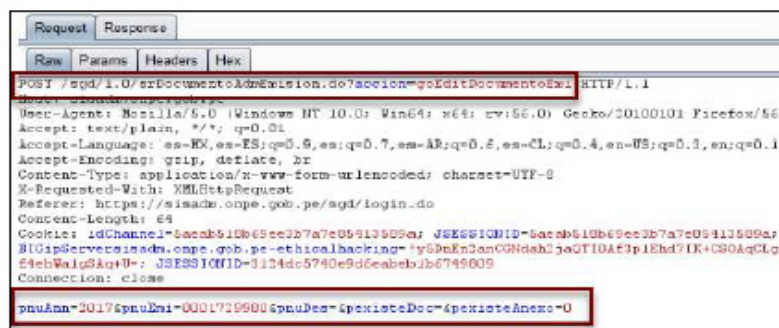
En la evaluación realizada sobre el sistema de información de la organización, se identificó que este envía diversos parámetros a través del método POST, pudiendo luego un eventual atacante modificar para obtener acceso a secciones restringidas.

Pruebas sobre la sección DOCUMENTOS:

Para realizar las pruebas se realizaron las siguientes operaciones sobre el sistema de información:

1. Se acceso con el usuario ERAMIREZC
2. Accede a la sección DOCUMENTOS
3. Se accede a la sección EMISION DE DOCUMENTOS y se obtiene el listado de documentos emitidos.
4. Se selecciona un documento del listado y se da clic en la opción EDITAR.

Se obtiene la siguiente petición:



Allí se puede identificar el parámetro PNUEMI, el mismo que contiene un valor identificativo de la emisión.

5. Se ingresa con el usuario NESPIRITU
6. Se coloca la petición identificada en el paso 04 y se accede a información no permitida.

Como resultado de las pruebas, es posible acceder al detalle de los documentos emitidos por otros usuarios del sistema de información sin contar con los privilegios para acceder a estos.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 24 de 78

Evidencia:

Fig12. Evidencia que el usuario NESPIRITU no tiene acceso al nro. de emisión 4413

Evidencia

Fig13. Evidencia de acceso NO autorizado a información a través de la manipulación de parámetros por el usuario NESPIRITU

Inadecuada Gestión de Privilegios: Acceso no autorizado al detalle de los documentos emitidos/recepcionados sección DOCUMENTOS.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS –	Código: EH-ONPE-IT
	FUNC 2017	Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 25 de 76

Evidencia

Request
Response

Raw
Params
Headers
Hex

POST /sgd/1.0/srDocumentoAdminExision.do?action=goEditDocumentoExi HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/plain, */*; q=0.01
Accept-Language: es-IX,es-ES;q=0.9,es;q=0.7,es-AR;q=0.6,es-CL;q=0.4,en-US;q=0.3,en;q=0.1
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://sisadu.onpe.gob.pe/sgd/login.do
Content-Length: 64
Cookie: jsChannel=5aeab518b69ee3b7a7e85413589a; JSESSIONID=5aeab518b69ee3b7a7e85413589a; BIGipServerisadu.onpe.gob.pe-ethicalhacking=!y5DnEnCanCjIdah2jaQTIOAf3pi2nd7IK+CSQaQLgJAGp; f4ehWaiGSAq+U=; JSESSIONID=3124dc5740e9d6eabebdb6749505
Connection: close

pruánn=CG17spnuEnl=0001729580spuaDes=apexiateDoc=apexiate&nexo=0

Fig14. Evidencia de acceso NO autorizado a información a través de la manipulación de parámetros por el usuario NESPIRITU

Sistema Vulnerable:

Nro.	Sistema de Información	Proceso Vulnerable
1	Sistema de Gestión Documental	Sección DOCUMENTOS

Valoración del Riesgo de la Vulnerabilidad.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017		Código: EH-ONPE -IT
	Informe Técnico – Primer Escaneo		Versión: 3.0
			Fecha: 03/10/17
			Página: 27 de 76

Valoración del Riesgo:

A continuación, se muestran los resultados de la valoración del riesgo de seguridad de información basada en el estándar CVSS (Common Vulnerability Scoring System):

Métricas de Puntuación Base	
Métricas de Explotabilidad	
Vector de Acceso	Remoto
Complejidad de Acceso	Medio
Autenticación requerida	Única
Métricas de Impacto	
Impacto en la confidencialidad	Completo
Impacto en la integridad	Parcial
Impacto en la disponibilidad	Parcial
Métricas de Puntuación Temporal	
Acceso a exploit	No definido
Corrección de vulnerabilidad disponible	No definido
Nivel de confiabilidad de la existencia de vulnerabilidad	No definido
Métricas de Puntuación del Entorno	
Potencial peligro colateral	No definido
Porcentaje distribuido de sistemas vulnerables	No definido

Resultados	
Puntuación Base CVSS	7.5
Subpuntuación de Impacto	8.5
Subpuntuación de Explotabilidad	6.8
Puntuación Temporal CVSS	No definido
Puntuación del Entorno CVSS	No definido
Puntuación Promedio CVSS	7.5

Inadecuada Gestión de Privilegios: Acceso no autorizado al detalle de los documentos emitidos/recepcionados sección MESA DE PARTES.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE-IT Versión: 3.0 Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 28 de 76

3.4. Inadecuada Gestión Privilegios: Acceso NO autorizado al detalle de documentos recepcionados por usuarios (sección MESA DE PARTES)

Descripción:

Durante el proceso de evaluación e identificación de vulnerabilidades, se realizaron pruebas de MANIPULACIÓN DE PARÁMETROS del sistema de información. La manipulación de parámetros tiene por objetivo obtener acceso y/o modificar solicitudes (REQUEST) del sistema de información para acceder a secciones restringidas o realizar operaciones sobre el sistema de información.

En la evaluación realizada sobre el sistema de información de la organización, se identificó que este envía diversos parámetros a través del método POST, pudiendo luego un eventual atacante modificar para obtener acceso a secciones restringidas.

Pruebas sobre la sección MESA DE PARTES:

1. Se accede con el usuario DBARRIOS, este usuario cuenta con el perfil MESA DE PARTES
2. Se ingresa la opción MESA DE PARTES y se obtiene un listado de los documentos que han sido RECEPCIONADOS.
3. Para el ejemplo, se ha recepcionado un documento del remitente "PALOMINO HUAMANÍ, OMAR MARTIN".



4. Se ingresa con el usuario NESPIRITU el cual tiene el perfil BASICO. Este usuario no tiene la opción mesa de partes.
5. Se coloca directamente la URL de edición de los documentos registrados en mesa de partes y es posible acceder a los mismos.
6. Además, se identificó que el mismo proceso se puede realizar para el proceso de creación de documentos de mesa de partes e inclusive es posible cambiar el estado de documento a REGISTRADO.

Inadecuada Gestión de Privilegios: Acceso no autorizado al detalle de los documentos emitidos/recepcionados sección MESA DE PARTES.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
		Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 29 de 76

Evidencia:

Evidencia



Fig15. Evidencia de acceso a información de MESA DE PARTES por el usuario DBARRIOS

Evidencia

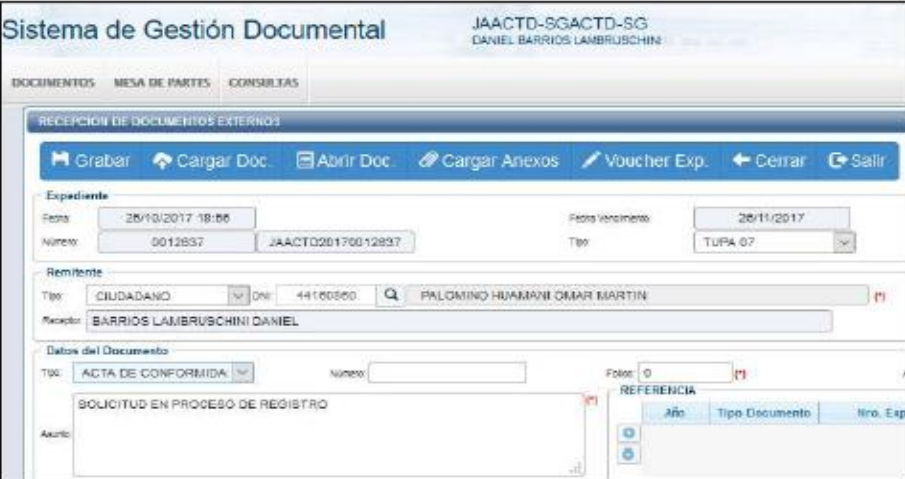


Fig16. Evidencia de acceso a información de MESA DE PARTES por el usuario DBARRIOS

Inadecuada Gestión de Privilegios: Acceso no autorizado al detalle de los documentos emitidos/recepcionados sección MESA DE PARTES.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE-IT Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17 Página: 30 de 78

Evidencia

[illegible]

Fig17. Evidencia de acceso NO autorizado a información a través de la manipulación de parámetros por el usuario NESPIRITU

Evidencia

[illegible]

Fig18. Evidencia de acceso NO autorizado a información a través de la manipulación de parámetros por el usuario NESPIRITU

Inadecuada Gestión de Privilegios: Acceso no autorizado al detalle de los documentos emitidos/recepcionados sección MESA DE PARTES.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
		Fecha: 03/10/17
Informe Técnico – Primer Escaneo		Página: 31 de 78

Evidencia

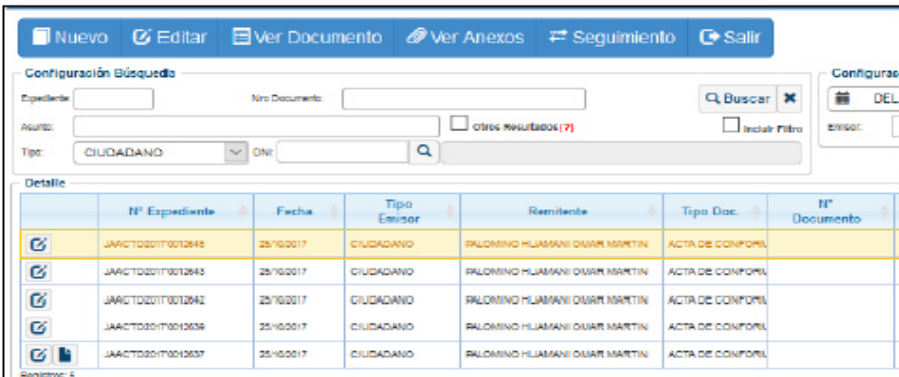


Fig19. Evidencia de acceso NO autorizado a información a través de la manipulación de parámetros por el usuario NESPIRITU – Creación de documentos de MESA DE PARTES

Evidencia

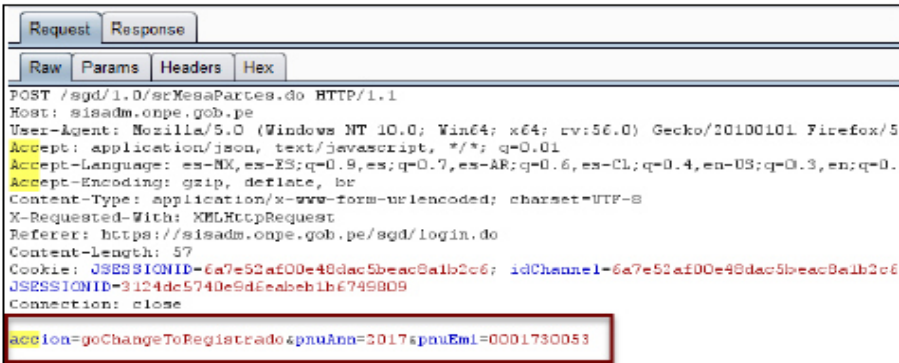


Fig20. Evidencia de acceso NO autorizado a información a través de la manipulación de parámetros por el usuario NESPIRITU – Creación de documentos de MESA DE PARTES

Sistema Vulnerable:

Nro.	Sistema de Información	Proceso Vulnerable
1	Sistema de Gestión Documental	Sección MESA DE PARTES

Valoración del Riesgo de la Vulnerabilidad.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
		Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 33 de 76

Valoración del Riesgo:

A continuación, se muestran los resultados de la valoración del riesgo de seguridad de información basada en el estándar CVSS (Common Vulnerability Scoring System):

Métricas de Puntuación Base	
Métricas de Explotabilidad	
Vector de Acceso	Remoto
Complejidad de Acceso	Medio
Autenticación requerida	Única
Métricas de Impacto	
Impacto en la confidencialidad	Completo
Impacto en la integridad	Parcial
Impacto en la disponibilidad	Parcial
Métricas de Puntuación Temporal	
Acceso a exploit	No definido
Corrección de vulnerabilidad disponible	No definido
Nivel de confiabilidad de la existencia de vulnerabilidad	No definido
Métricas de Puntuación del Entorno	
Potencial peligro colateral	No definido
Porcentaje distribuido de sistemas vulnerables	No definido

Resultados	
Puntuación Base CVSS	7.5
Subpuntuación de Impacto	8.5
Subpuntuación de Explotabilidad	6.8
Puntuación Temporal CVSS	No definido
Puntuación del Entorno CVSS	No definido
Puntuación Promedio CVSS	7.5

Inadecuada Gestión de Privilegios: Recepción de documentos de manera no autorizada.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 34 de 76

3.5. Inadecuada Gestión de Privilegios: Recepción de documentos de manera NO autorizada

Descripción:

Durante el proceso de evaluación e identificación de vulnerabilidades, se realizaron pruebas de MANIPULACIÓN DE PARÁMETROS del sistema de información. La manipulación de parámetros tiene por objetivo obtener acceso y/o modificar solicitudes (REQUEST) del sistema de información para acceder a secciones restringidas o realizar operaciones sobre el sistema de información.

En la evaluación realizada sobre el sistema de información de la organización, se identificó que este envía diversos parámetros a través del método POST, pudiendo luego un eventual atacante modificar para obtener acceso a secciones restringidas.

Pruebas sobre el proceso de RECEPCIÓN DE DOCUMENTOS:

Escenario 01:

Se realiza la emisión de un documento para el usuario NESPIRITU. Este documento solo puede ser recibido por él.

El usuario ERAMIREZC envía la petición de recepción de documento y en la bandeja de consultas de NESPIRITU se marca el documento como recibido.

Escenario 02:

Cualquier usuario conociendo la solicitud puede realizar la recepción de documentos en nombre de otro, suplantando su identidad del mismo.

Escenario 03:

Cualquier usuario puede recepcionar un documento que no le pertenece a través de la modificación de parámetros.

Evidencia:

Evidencia

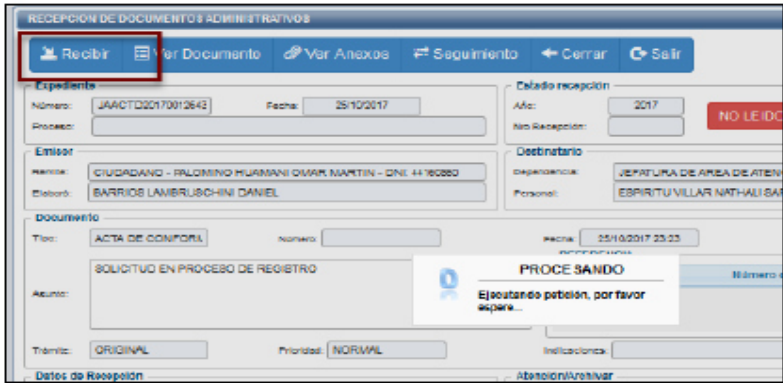


Fig21. Evidencia de envío de solicitud para obtener la petición en el proceso de RECIBIR un documento

Inadecuada Gestión de Privilegios: Recepción de documentos de manera no autorizada.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 35 de 76

Evidencia

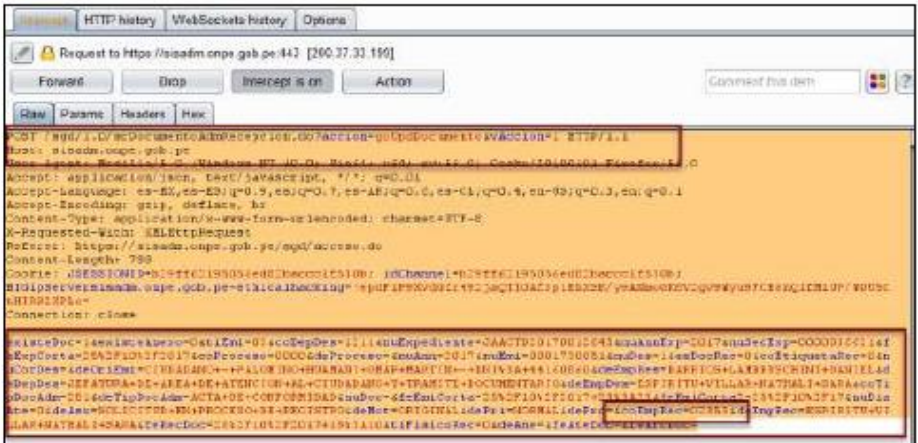


Fig22. Evidencia de obtención de parámetros obtenidos en el proceso de RECIBIR documento, allí se obtiene el parámetro EMPREC

Evidencia

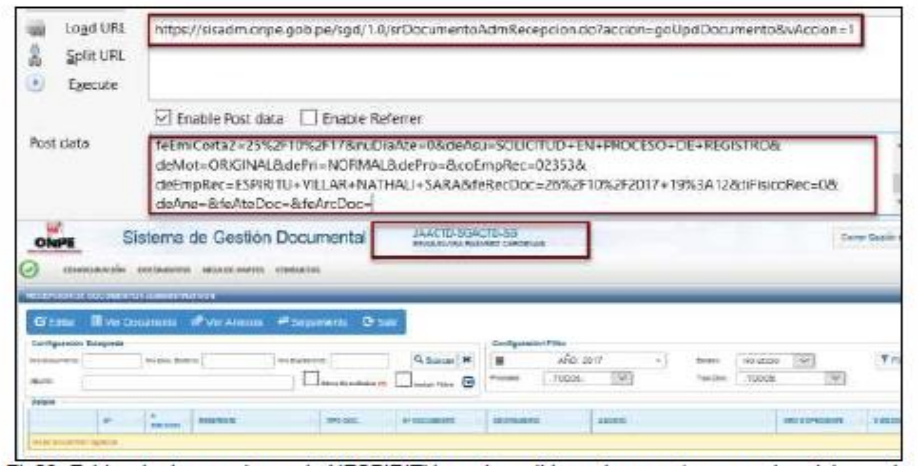


Fig23. Evidencia de que el usuario NESPIRITU puede recibir un documento en nombre del usuario DBARRIOS

Inadecuada Gestión de Privilegios: Recepción de documentos de manera no autorizada.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017		Código: EH-ONPE -IT
	Informe Técnico – Primer Escaneo		Versión: 3.0
			Fecha: 03/10/17
			Página: 36 de 76

Evidencia

Log URL

Split URL

Execute

<https://sisadm.onpe.gob.pe/sgd/1.0/srDocumentoAdmRecepcion.do?accion=goUpdDocumento&vAccion=1>

☒ Enable Post data ☐ Enable Referrer

Post data

```
feEmiCorta2=25%2F10%2F17&nuDiaAte=0&deAsu=SOLICITUD+EN+PROCESO+DE+REGISTRO&
deMot=ORIGINAL&dePri=NORMAL&dePro=&coEmpRec=02353&
deEmpRec=ESPIRITU+VILLAR+NATHALI+SARA&feRecDoc=26%2F10%2F2017+19%3A12&tiFisicoRec=0&
deAne=&feAteDoc=&feArcDoc=
```

```
("coResponse":"1","deResponse":"OK","seCodDoc":"7290","seDecRec":"1","deEdDecRec":"RECIBIDO")
```

Fig24. Evidencia de recepción de documento por el usuario NESPIRITU suplantando la identidad de DBARRIOS.

Sistema Vulnerable:

Nro.	Sistema de Información	Proceso Vulnerable
1	Sistema de Gestión Documental	Proceso de RECEPCIÓN DE DOCUMENTOS

Valoración del Riesgo de la vulnerabilidad.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
		Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 38 de 76

Valoración del Riesgo:

A continuación, se muestran los resultados de la valoración del riesgo de seguridad de información basada en el estándar CVSS (Common Vulnerability Scoring System):

Métricas de Puntuación Base	
Métricas de Explotabilidad	
Vector de Acceso	Remoto
Complejidad de Acceso	Medio
Autenticación requerida	Única
Métricas de Impacto	
Impacto en la confidencialidad	Completo
Impacto en la integridad	Parcial
Impacto en la disponibilidad	Parcial
Métricas de Puntuación Temporal	
Acceso a exploit	No definido
Corrección de vulnerabilidad disponible	No definido
Nivel de confiabilidad de la existencia de vulnerabilidad	No definido
Métricas de Puntuación del Entorno	
Potencial peligro colateral	No definido
Porcentaje distribuido de sistemas vulnerables	No definido

Resultados	
Puntuación Base CVSS	7.5
Subpuntuación de Impacto	8.5
Subpuntuación de Explotabilidad	6.8
Puntuación Temporal CVSS	No definido
Puntuación del Entorno CVSS	No definido
Puntuación Promedio CVSS	7.5

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT Versión: 3.0 Fecha: 03/10/17 Página: 39 de 76
	Informe Técnico – Primer Escaneo	

3.6. Inadecuada Gestión de Privilegios: Carga/modificación de documentos de manera NO autorizada.

Descripción:

Durante el proceso de evaluación e identificación de vulnerabilidades, se realizaron pruebas de MANIPULACIÓN DE PARÁMETROS del sistema de información. La manipulación de parámetros tiene por objetivo obtener acceso y/o modificar solicitudes (REQUEST) del sistema de información para acceder a secciones restringidas o realizar operaciones sobre el sistema de información.

En la evaluación realizada sobre el sistema de información de la organización, se identificó que este envía diversos parámetros a través del método POST, pudiendo luego un eventual atacante modificar para obtener acceso a secciones restringidas.

Pruebas sobre el proceso de CARGA DE DOCUMENTOS:

- Acceso a la sección de emisión de documentos con cualquier USUARIO.
- Al realizar la carga de un documento se genera la siguiente petición (REQUEST).


```
POST /sgd/i.o/es/DocumentsAdministrar.do HTTP/1.1
Host: saadm.onpe.gob.pe
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/plain,*/* q=0.01
Accept-Language: es-ES,es;q=0.9,en;q=0.7,es-AE;q=0.6,es-GU;q=0.4,es-US;q=0.3,es;q=0.1
Accept-Encoding: gzip, deflate, br
Accept-Charset: utf-8,utf-16,utf-32;q=0.7,*/* q=0.1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://saadm.onpe.gob.pe/sgd/login.do
Cookie: JSESSIONID=425077244B8B0A5C0A17490B02; 1dChannel=425077244B8B0A5C0A17490B02; BIGipServeronpe.onpe.gob.pe-ethicalhacking=1f1f1decyptT0RtCjA2TG0At3pIEZnsm8Hq3CteRelteF8MzEd3Jh+e3J2AGMLBg[9]WVW/g; JSESSIONID=1124d5740edfeeb01bd748DCE
Connection: close
ccpccgpcCargadoIniciando=2017IndId=00017330354csOps=4IndId=201703027330354G64402-putIndId=2017ACTA-R1626-2017-EPC-2-UTD-SSACFD-SG.pdf
```

- En la petición (REQUEST) se puede identificar los siguientes valores:
 - Tipo de documento
 - Asunto
 - Destinatario
- Un eventual atacante del sistema de información realiza la generación del documento en formato PDF en repositorio.
- Finalmente, se realiza la carga del documento PDF generado en el paso anterior modificando los parámetros identificados en el paso 02.

Como resultado de las pruebas se identificó lo siguiente:

- Un eventual atacante puede realizar la carga de archivos de manera no autorizada en el cualquier proceso de EMISIÓN, para realizar esto el atacante sólo debe modificar el parámetro "NUEMI" a través de técnicas de fuzzing.
- En las evidencias mostradas a continuación, se realiza la modificación del parámetro "NUEMI" y se logra modificar el documento cargado en el proceso de EMISIÓN.

SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017		Código: EH-ONPE-IT
		Versión: 3.0
		Fecha: 03/10/17
		Página: 40 de 76

Informe Técnico – Primer Escaneo

Evidencia:

Evidencia

Fig25. Evidencia de la carga de archivos a través de la manipulación de parámetros.

Evidencia

Fig26. Evidencia de la carga de archivos a través de la manipulación de parámetros.

Sistema Vulnerable:

Nro.	Sistema de Información	Proceso Vulnerable
1	Sistema de Gestión Documental	Proceso de RECEPCION DE DOCUMENTOS

Valoración del Riesgo de la Vulnerabilidad.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
		Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 42 de 76

Valoración del Riesgo:

A continuación, se muestran los resultados de la valoración del riesgo de seguridad de información basada en el estándar CVSS (Common Vulnerability Scoring System):

Métricas de Puntuación Base	
Métricas de Explotabilidad	
Vector de Acceso	Remoto
Complejidad de Acceso	Medio
Autenticación requerida	Única
Métricas de Impacto	
Impacto en la confidencialidad	Completo
Impacto en la integridad	Parcial
Impacto en la disponibilidad	Parcial
Métricas de Puntuación Temporal	
Acceso a exploit	No definido
Corrección de vulnerabilidad disponible	No definido
Nivel de confiabilidad de la existencia de vulnerabilidad	No definido
Métricas de Puntuación del Entorno	
Potencial peligro colateral	No definido
Porcentaje distribuido de sistemas vulnerables	No definido

Resultados	
Puntuación Base CVSS	7.5
Subpuntuación de Impacto	8.5
Subpuntuación de Explotabilidad	6.8
Puntuación Temporal CVSS	No definido
Puntuación del Entorno CVSS	No definido
Puntuación Promedio CVSS	7.5

Formulario de acceso al sistema susceptible a ataques recurrentes de acceso.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE-IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 43 de 76

3.7. Formulario de acceso al sistema susceptible a ataques recurrentes de acceso.

Descripción:

Durante el proceso de evaluación de vulnerabilidades en CAJA NEGRA, se identificó que el sistema de información no cuenta con un control ante ataques recurrentes en el formulario de acceso al mismo.

Los ataques de acceso recurrente tienen las dos siguientes características:

1. Ataques de fuerza bruta de manera indeterminada
2. Ataques de diccionario en base a patrones de contraseñas
3. Ataques controlados de un solo intento (una sola contraseña) sobre todos los usuarios de la organización.

El equipo consultor de KUNAK Consulting realizó ataques controlados de un solo intento sobre el sistema de información e identificó las siguientes características:

1. Los usuarios y contraseñas son enviados con un mecanismo de ofuscación.
2. El mecanismo es implementado a través de librerías JAVASCRIPT.
3. Finalmente, como el mecanismo utilizado siempre es el mismo es posible identificar los usuarios y contraseñas enviadas, es decir, basta con identificar una sola vez el usuario enviado y a través de esto se puede realizar el ataque de fuerza bruta.

Como resultado de las pruebas, se realizó un ataque de un (01) intento y posible identificar el mecanismo de ofuscación utilizado por el sistema de información:

Evidencia:

Evidencia

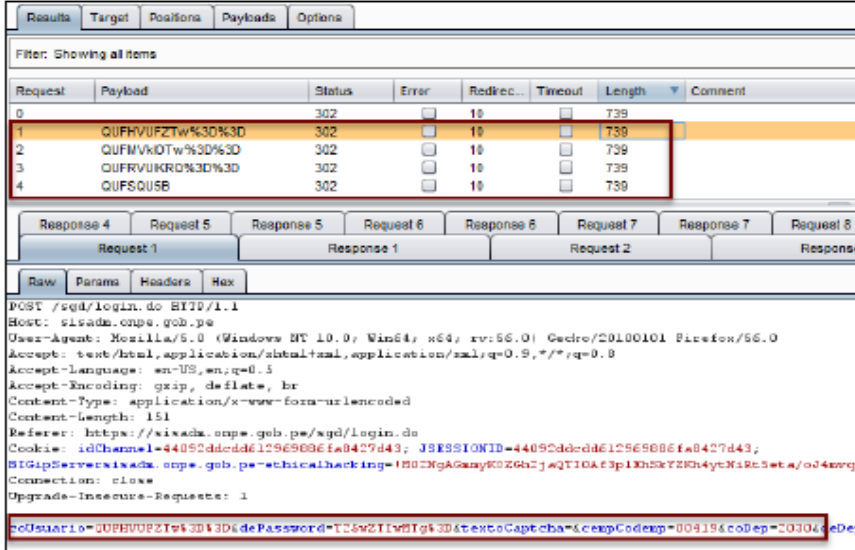


Fig27. Evidencia de ataque recurrente sobre el formulario de acceso a la organización

Formulario de acceso al sistema susceptible a ataques recurrentes de acceso.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 44 de 76

Nro.	Usuario	Contraseña ofuscada
1	AA	QUFHVUFZTw%3D%3D
2	AA	QUFMVkiOTw%3D%3D
3	AA	QUFRVUIKRQ%3D%3D
4	AA	QUFSQU5B
5	AA	QUFUT0NIRQ%3D%3D
6	AB	QUJFQ0VSUkE%3D
7	AC	QUNBQ0VSRVM%3D
8	AC	QUNBTkNJt8%3D
9	AC	QUNBU1RJTEXP
10	AC	QUNIQVZFwG%3D%3D
11	AF	QUZMT1JFUw%3D%3D
12	AG	QUdBTUFSUkE%3D
13	AI	QUIOR0E%3D
14	AL	QUxFVkfOTw%3D%3D
15	AL	QUxJQkVSQVRP
16	AM	QU1BUkFWSQ%3D%3D
17	AM	QU1BWVRB
18	AM	QU1FWkE%3D
19	AM	QU1PUkFMRVM%3D
20	AM	QU1PUk%3D
21	AP	QVBFUkVa
22	AP	QVBPTUE%3D
23	AP	QVBVQ0NJTw%3D%3D
24	AQ	QVFVSU5UQU5JTExB
25	AQ	QVFVSVNQVRVY%3D
26	AS	QVNVWU90
27	AV	QVZBTERJVkIB
28	AV	QVZFTEFSREU%3D
29	AZ	QVpFVkfMTE9T
30	BB	QkJPtFVBUIRF
31	BC	QkNVRVZB
32	BG	QkdBUkNFUw%3D%3D
33	BL	QkxPUEVa
34	BO	Qk9ST1NDTw%3D%3D
35	BP	QIBBUkRP
36	BP	QIBPUIRPQ0FSUkVSTw%3D%3D
37	BR	QIJFWU5B
38	BS	QINFQ0xFTg%3D%3D
39	CA	Q0FDRVZFRE8%3D
40	CA	Q0FHVUISUkU%3D
41	CA	Q0FHVUISUkVI
42	CAL	Q0FMVkfSQURP
43	CAP	Q0FQVJJQ0IP
44	CAR	Q0FSUIVOQVRFR1VJ
45	CBE	Q0JFT1VUSVM%3D
46	CC	Q0NBukRP
47	CCA	Q0NBUIBTIpB
48	CCC	Q0NPukRPV%3D
49	CFI	Q0ZMT1JFUw%3D%3D
50	CG	Q0dBUkNJQQ%3D%3D
51	CG	Q0dPTUvA
52	CGU	Q0dVVEIFUIJFWG%3D%3D
53	CM	Q01PTIRFUw%3D%3D
54	CNA	Q05BVkFSUk9D
55	COF	Q09SRUxMQU5B
56	CPA	Q1BBTE9NSU5P
57	CF	Q1BFUkFMVEE%3D
58	CF	Q1JBTU8T
59	C	Q1JJU0NP

Valoración del Riesgo de la Vulnerabilidad.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017		Código: EH-ONPE -IT
	Informe Técnico – Primer Escaneo		Versión: 3.0
			Fecha: 03/10/17
			Página: 51 de 76

Valoración del Riesgo:

A continuación, se muestran los resultados de la valoración del riesgo de seguridad de información basada en el estándar CVSS (Common Vulnerability Scoring System):

Métricas de Puntuación Base	
Métricas de Explotabilidad	
Vector de Acceso	Remoto
Complejidad de Acceso	Medio
Autenticación requerida	Ninguna
Métricas de Impacto	
Impacto en la confidencialidad	Parcial
Impacto en la integridad	Ninguno
Impacto en la disponibilidad	Ninguno
Métricas de Puntuación Temporal	
Acceso a exploit	No definido
Corrección de vulnerabilidad disponible	No definido
Nivel de confiabilidad de la existencia de vulnerabilidad	No definido
Métricas de Puntuación del Entorno	
Potencial peligro colateral	No definido
Porcentaje distribuido de sistemas vulnerables	No definido
Resultados	
Puntuación Base CVSS	4.3
Subpuntuación de Impacto	2.9
Subpuntuación de Explotabilidad	8.6
Puntuación Temporal CVSS	No definido
Puntuación del Entorno CVSS	No definido
Puntuación Promedio CVSS	4.3

Formulario de acceso permite la enumeración de usuarios del sistema de información.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017		Código: EH-ONPE -IT
	Informe Técnico – Primer Escaneo		Versión: 3.0
			Fecha: 03/10/17
			Página: 52 de 76

3.8. Formulario de acceso permite la enumeración de usuarios del sistema de información

Descripción:

Mediante la revisión y análisis de vulnerabilidades sobre el formulario de acceso al sistema de información, se identificó que el formulario permite realizar la enumeración de usuarios que se encuentran registrados en el sistema.

El proceso de enumeración de usuarios resulta crítico cuando se realizan análisis de vulnerabilidades sobre el sistema, esto debido que permite identificar aquellos usuarios que se encuentran registrados en el sistema y sobre estos realizar ataques de acceso no autorizado como se realizaron en este informe en la sección “3.7. Formulario de acceso al sistema susceptible a ataques recurrentes de acceso”.

Como resultado de las pruebas, se identificó lo siguiente:

Si se coloca un usuario que EXISTE se obtiene: Se carga la DEPENDENCIA a la que pertenece.

Si se coloca un usuario que NO EXISTE se obtiene: USUARIO NO TIENE ACCESO AL SISTEMA

En base al proceso de enumeración fue posible identificar 360 usuarios del sistema de información.

Riesgo de Seguridad:

1. Un eventual atacante identifica los usuarios del sistema de información a través de revisiones manuales.
2. Con los usuarios identificados en el paso 01, el atacante realiza un ataque de fuerza bruta sobre el usuario hasta lograr ingresar al sistema de información.

Evidencia:

Evidencia



Fig28. Evidencia enumeración de cuentas de usuarios en el sistema

Formulario de acceso permite la enumeración de usuarios del sistema de información.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
		Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 53 de 76

Evidencia



Sistema de Gestión Documental

Usuario

ERAMIREZC

Contraseña

Dependencia

JEFATURA DE AREA DE ATENCION A 

Ingresar

[Requisitos del sistema](#) [Manual de usuario](#)

Fig29. Evidencia enumeración de cuentas de usuarios en el sistema

Formulario de acceso permite la enumeración de usuarios del sistema de información.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
		Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 54 de 76

Nro.	Usuario	Código Empleado	Código Departamento	Nombre de Departamento	Número de Intento	Número de intentos realizados	Número de intento máximo
1		'coEmp'	'coDep'	'deDep'.JEFATURA DE AREA DE ARCHIVO ELECTORAL Y VERIFICACION DE FIRMAS	'nuint'	'0'	'nuintMaxCapit.'5'
2		'coEmp'	'coDep'	'deDep'.SUB GERENCIA DE FINANZAS	'nuint'	'0'	'nuintMaxCapit.'5'
3		'coEmp'	'coDep'	'deDep'.SUB GERENCIA DE ASESORIA ADMINISTRATIVA	'nuint'	'0'	'nuintMaxCapit.'5'
4		'coEmp'	'coDep'	'deDep'.OFICINA REGIONAL DE COORDINACION PUCALLPA	'nuint'	'0'	'nuintMaxCapit.'5'
5		'coEmp'	'coDep'	'deDep'.JEFATURA DE AREA DE NORMATIVA Y REGULACION DE FINANZAS PARTIDARIAS	'nuint'	'0'	'nuintMaxCapit.'5'
6		'coEmp'	'coDep'	'deDep'.SUB GERENCIA DE RECURSOS HUMANOS	'nuint'	'0'	'nuintMaxCapit.'5'
7		'coEmp'	'coDep'	'deDep'.SUB GERENCIA DE RELACIONES CORPORATIVAS	'nuint'	'0'	'nuintMaxCapit.'5'
8		'coEmp'	'coDep'	'deDep'.GERENCIA DE GESTION ELECTORAL	'nuint'	'1'	'nuintMaxCapit.'5'
9		'coEmp'	'coDep'	'deDep'.JEFATURA NACIONAL	'nuint'	'0'	'nuintMaxCapit.'5'
10		'coEmp'	'coDep'	'deDep'.OFICINA REGIONAL DE COORDINACION ICA	'nuint'	'0'	'nuintMaxCapit.'5'
11		'coEmp'	'coDep'	'deDep'.SUB GERENCIA DE OPERACIONES INFORMATICAS	'nuint'	'0'	'nuintMaxCapit.'5'
12		'coEmp'	'coDep'	'deDep'.JEFATURA DE AREA DE ARCHIVO ELECTORAL Y VERIFICACION DE FIRMAS	'nuint'	'0'	'nuintMaxCapit.'5'
13		'coEmp'	'coDep'	'deDep'.JEFATURA DE AREA DE PLATAFORMA TECNOLOGICA	'nuint'	'0'	'nuintMaxCapit.'5'
14		'coEmp'	'coDep'	'deDep'.JEFATURA DE AREA DE PLATAFORMA TECNOLOGICA	'nuint'	'1'	'nuintMaxCapit.'5'
15		'coEmp'	'coDep'	'deDep'.JEFATURA DE AREA DE VERIFICACION Y CONTROL	'nuint'	'0'	'nuintMaxCapit.'5'
16		'coEmp'	'coDep'	'deDep'.OFICINA REGIONAL DE COORDINACION CAJAMARCA	'nuint'	'0'	'nuintMaxCapit.'5'
17		'coEmp'	'coDep'	'deDep'.SUB GERENCIA DE COMUNICACIONES Y PRENSA	'nuint'	'0'	'nuintMaxCapit.'5'
18		'coEmp'	'coDep'	'deDep'.SUB GERENCIA DE FORMACION Y CAPACITACION ELECTORAL	'nuint'	'0'	'nuintMaxCapit.'5'
19		'coEmp'	'coDep'	'deDep'.PROCURADURIA PUBLICA	'nuint'	'0'	'nuintMaxCapit.'5'
20		'coEmp'	'coDep'	'deDep'.SUB GERENCIA DE RELACIONES CORPORATIVAS	'nuint'	'0'	'nuintMaxCapit.'5'
21		'coEmp'	'coDep'	'deDep'.OFICINA REGIONAL DE COORDINACION TRUJILLO	'nuint'	'0'	'nuintMaxCapit.'5'
22		'coEmp'	'coDep'	'deDep'.GERENCIA DE GESTION ELECTORAL	'nuint'	'0'	'nuintMaxCapit.'5'
23		'coEmp'	'coDep'	'deDep'.PROCURADURIA PUBLICA	'nuint'	'0'	'nuintMaxCapit.'5'
24		'coEmp'	'coDep'	'deDep'.SUB GERENCIA DE ASISTENCIA TECNICA	'nuint'	'0'	'nuintMaxCapit.'5'
25		'coEmp'	'coDep'	'deDep'.SUB GERENCIA DE ORGANIZACION ELECTORAL DESCONCENTRADA	'nuint'	'0'	'nuintMaxCapit.'5'

Valoración del Riesgo de la Vulnerabilidad.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 69 de 76

Valoración del Riesgo:

A continuación, se muestran los resultados de la valoración del riesgo de seguridad de información basada en el estándar CVSS (Common Vulnerability Scoring System):

Métricas de Puntuación Base	
Métricas de Explotabilidad	
Vector de Acceso	Remoto
Complejidad de Acceso	Medio
Autenticación requerida	Ninguna
Métricas de Impacto	
Impacto en la confidencialidad	Parcial
Impacto en la integridad	Ninguno
Impacto en la disponibilidad	Ninguno
Métricas de Puntuación Temporal	
Acceso a exploit	No definido
Corrección de vulnerabilidad disponible	No definido
Nivel de confiabilidad de la existencia de vulnerabilidad	No definido
Métricas de Puntuación del Entorno	
Potencial peligro colateral	No definido
Porcentaje distribuido de sistemas vulnerables	No definido
Resultados	
Puntuación Base CVSS	4.3
Subpuntuación de Impacto	2.9
Subpuntuación de Explotabilidad	8.6
Puntuación Temporal CVSS	No definido
Puntuación del Entorno CVSS	No definido
Puntuación Promedio CVSS	4.3

Identificación de información innecesaria transferida en las solicitudes enviadas en el sistema de Gestión Documental.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
	Informe Técnico – Primer Escaneo	Fecha: 03/10/17
		Página: 70 de 76

3.9. Identificación de información innecesaria transferida en las solicitudes enviadas en el sistema de información

Descripción:

Como parte de las pruebas realizadas en CAJA NEGRA sobre el formulario de acceso al sistema de información, fue posible identificar RESPUESTAS al proceso que accede que envían información sensible que un eventual atacante puede utilizar para realizar ataques de mayor complejidad.

Para identificar la vulnerabilidad y la información innecesaria identificada se deben realizar los siguientes pasos:

1. Se accede al sistema de información.
2. Se ingresa un usuario válido en el sistema y el sistema envía información de acceso.
3. Al evaluar la respuesta del servidor, se puede identificar la siguiente información:
 - a. Código de Empleado
 - b. Código de Departamento
 - c. Nombre de Departamento
 - d. Número de intentos fallidos realizados.
 - e. Número de intentos máximos permitidos

Riesgo de Seguridad:

La información identificada representa un riesgo de seguridad debido a lo siguiente:

1. El atacante ya conoce el número de intentos máximos permitidos.
2. El atacante ya conoce cuantos intentos fallidos han realizado. Es importante mencionar que esta información puede ser obtenida del DIRECTORIO ACTIVO de la organización lo cual representa un riesgo mayor inclusive.
3. Además, permite identificar el periodo de tiempo en el cual el conteo de intentos fallidos vuelve a su cuenta inicial, es decir, a un valor cero.
4. Finalmente, con los valores de CÓDIGO DE EMPLEADO y CÓDIGO DE DEPARTAMENTO es posible realizar la modificación de parámetros en base a las vulnerabilidades descritas en:
 - a. Inadecuada Gestión de Privilegios: Acceso NO autorizado al detalle de documentos emitidos/recepcionados por usuarios (sección CONSULTAS)
 - b. Inadecuada Gestión de Privilegios: Acceso NO autorizado al detalle de documentos emitidos/recepcionados por usuarios (sección DOCUMENTOS)
 - c. Inadecuada Gestión de Privilegios: Acceso NO autorizado al detalle de documentos recepcionados por usuarios (sección MESA DE PARTES).
 - d. Inadecuada Gestión de Privilegios: Recepción de documentos de manera NO autorizada.
 - e. Inadecuada Gestión de Privilegios: Carga/modificación de documentos de manera NO autorizada.

Identificación de información innecesaria transferida en las solicitudes enviadas en el sistema de Gestión Documental.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017		Código: EH-ONPE -IT
	Informe Técnico – Primer Escaneo		Versión: 3.0
			Fecha: 03/10/17
			Página: 71 de 76

Evidencia:

Evidencia

Request
Response

Raw
Params
Headers
Hex

```

POST /sgd/1.0/sgDepAcceso.do HTTP/1.1
Host: sisadm.onpe.gob.pe
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/plain, */*; q=0.01
Accept-Language: es-MX,es-ES;q=0.9,es;q=0.7,es-AR;q=0.6,es-CL;q=0.4,en-US;q=0.3,en;q=0.1
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://sisadm.onpe.gob.pe/sgd/login.do
Content-Length: 43
Cookie: JSESSIONID=cb3175b44620cfd7a8758a410c81; idChannel=cb3175b44620cfd7a8758a410c81; BIGipServerssisadm.onpe.gob.pe-ethicalhacking=!Gm18K/AvCec928J2jaQT10Af3p1EhfL00 +NExecTf1ehtA6QxWA6x2wQ7r4uKB23WQs99jUPHTG+KTU=; JSESSIONID=dfa22ee334bd35b72c98f18eef4d
Connection: close

accion=goSeleccionaDep&pcoUsuario=ERANIREZC
        
```

Fig30. Evidencia de identificación de REQUEST en donde se envía el identificador del usuario

Evidencia

Request
Response

Raw
Headers
Hex

```

HTTP/1.1 200 OK
Server: GlassFish Server Open Source Edition 4.1
X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition 4.1 Java/Oracle Corporation/1.8)
X-FRAME-OPTIONS: DENT
Content-Type: text/plain; charset=ISO-8859-1
Date: Fri, 27 Oct 2017 17:06:18 GMT
Connection: close
Content-Length: 167
Set-Cookie: BIGipServerssisadm.onpe.gob.pe-ethicalhacking=!GGS4924VEYxroPx2jaQT10Af3p1EhfL00 IzLk2/hKTeSBQCqQa2G6ZKkF80cVQ+3mYvTcVAA6m318Eg-; path=/; Httponly; Secure

({'retval':'OK','coEmp':'02298','coDep':'1211','deDep':'JEFATURA DE AREA DE ATENCION AL CIUDADANO Y TRAMITE DOCUMENTARIO','nuInt':'0','nuIntMax':'3','nuIntMaxCapt':'5'})
        
```

Fig31. Evidencia de información innecesaria enviada como respuesta al ingreso de usuarios

Valoración del Riesgo de la Vulnerabilidad.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
		Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 73 de 76

Valoración del Riesgo:

A continuación, se muestran los resultados de la valoración del riesgo de seguridad de información basada en el estándar CVSS (Common Vulnerability Scoring System):

Métricas de Puntuación Base	
Métricas de Explotabilidad	
Vector de Acceso	Remoto
Complejidad de Acceso	Medio
Autenticación requerida	Ninguna
Métricas de Impacto	
Impacto en la confidencialidad	Parcial
Impacto en la integridad	Ninguno
Impacto en la disponibilidad	Ninguno
Métricas de Puntuación Temporal	
Acceso a exploit	No definido
Corrección de vulnerabilidad disponible	No definido
Nivel de confiabilidad de la existencia de vulnerabilidad	No definido
Métricas de Puntuación del Entorno	
Potencial peligro colateral	No definido
Porcentaje distribuido de sistemas vulnerables	No definido

Resultados	
Puntuación Base CVSS	4.3
Subpuntuación de Impacto	2.9
Subpuntuación de Explotabilidad	8.6
Puntuación Temporal CVSS	No definido
Puntuación del Entorno CVSS	No definido
Puntuación Promedio CVSS	4.3

Debilidades en las cabeceras del protocolo HTTP.

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
		Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 74 de 76

3.10. Debilidades en las cabeceras del protocolo HTTP

Descripción:

Los controles sobre cabeceras del protocolo HTTP brindan a los servidores web niveles de seguridad ante ataques que se realizan sobre los mismos. Estos controles pertenecen a la categoría de PREVENTIVOS, es decir, no permiten que los mismos sean ejecutados.

Los controles que son agregados a nivel de las cabeceras del protocolo HTTP son:

1. Controles ante ataques XSS (Cross Site Scripting)
2. Controles ante ataques MIME para exploradores Chrome e Internet Explorer
3. Controles para evitar ataques de suplantación de nombres a través de DNS, controles HSTS.

Además, se identificó exposición de información innecesaria asociada a la versión del servicio web GLASSFISH.

Se recomienda la implementación de estos controles a nivel de la configuración del servidor web y eliminar la información innecesaria de las cabeceras del protocolo HTTP.

Evidencia:

Evidencia

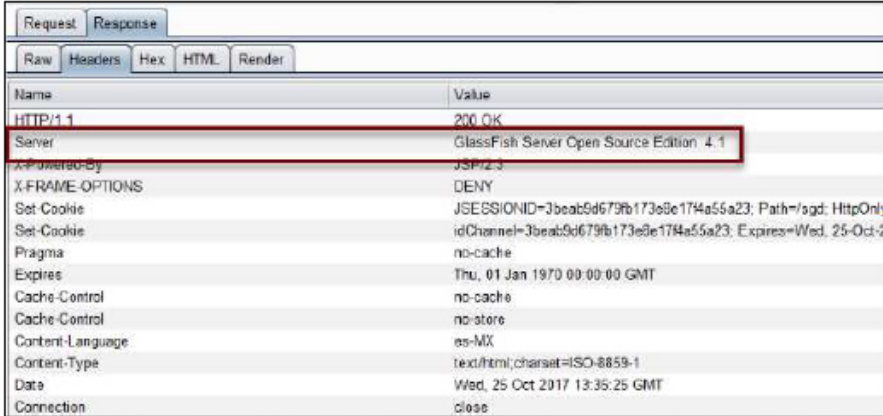


Fig32. Acceso de ausencia de controles de seguridad en las cabeceras del protocolo HTTP

Sistema Vulnerable:

Nro.	Sistema de Información
1	Sistema de Gestión Documental

Valoración del Riesgo de la Vulnerabilidad

	SERVICIO DE ETHICAL HACKING – SGD – CONVENIOS – FUNC 2017	Código: EH-ONPE -IT
		Versión: 3.0
		Fecha: 03/10/17
	Informe Técnico – Primer Escaneo	Página: 76 de 76

Valoración del Riesgo:

A continuación, se muestran los resultados de la valoración del riesgo de seguridad de información basada en el estándar CVSS (Common Vulnerability Scoring System):

Métricas de Puntuación Base	
Métricas de Explotabilidad	
Vector de Acceso	Remoto
Complejidad de Acceso	Bajo
Autenticación requerida	Ninguna
Métricas de Impacto	
Impacto en la confidencialidad	Parcial
Impacto en la integridad	Ninguno
Impacto en la disponibilidad	Ninguno
Métricas de Puntuación Temporal	
Acceso a exploit	Alto
Corrección de vulnerabilidad disponible	Solución Oficial
Nivel de confiabilidad de la existencia de vulnerabilidad	Confirmado
Métricas de Puntuación del Entorno	
Potencial peligro colateral	Bajo (Pérdida baja)
Porcentaje distribuido de sistemas vulnerables	Bajo (0-25%)

Resultados	
Puntuación Base CVSS	5.0
Subpuntuación de Impacto	2.9
Subpuntuación de Explotabilidad	10.0
Puntuación Temporal CVSS	4.4
Puntuación del Entorno CVSS	1.2
Puntuación Promedio CVSS	1.2

ANEXO 2 – PASE A CONTROL DE CALIDAD

Solicitud de Creación de Carpeta

Responder

Responder a todos

Reenviar



miércoles 08/08/2018 04:26 p.m.

Roxana Z. Cerda Alvarez

[SGD] Creación de Carpeta

Para

Williams B. Vargas Mamani

CC

Jose A. Vidal Estrada; Emilio Rojas Soria; Kenny A. Francia Augusto; Juan C. Calixto Salazar; Richard Cham Chen; Renzo S. Francia Marroquin



Mensaje enviado con importancia Alta.

Estimado Williams,

Se solicita la creación de la carpeta **PASCC-046-415** del Mantenimiento al Sistema de Gestión Documental, para subir el documento y archivo para la respectiva revisión.

Código: SG-415-2015-SGPEL-GITE/ONPE
Nombre: Mantenimiento al Sistema de Gestión Documental
Acceso a la Carpeta:

- ✓ Juan C. Calixto Salazar
- ✓ Richard Cham Chen
- ✓ Roxana Cerda Alvarez

Quedo a la espera de su confirmación.

Atentamente,

Roxana Z. Cerda Alvarez
Documentador de Aplicaciones
ONPE – GITE – SGPEL

Jr. Washington 1894, I Lima – Perú
Teléfono (511) 417 0630
www.onpe.gob.pe

Confirmación de Ruta de Carpeta Creada

 Responder  Responder a todos  Reenviar



miércoles 06/08/2018 04:53 p.m.

Jose A. Vidal Estrada

RE: [SGD] Creación de Carpeta

Para: Rosana Z. Cerda Alvarez

CC: Juan C. Calisto Salazar; Richard Chen-Chen; Williams E. Vargas Mamani

Ruta creada:

[\\gate-proyectos\PROYECTOS ONPE\STU\SG-415-2015\01_Pase a Control de Calidad\PASCC-046-415_08.08.2018](#)

Verificar accesos

Saludos



José Antonio Vidal Estrada

Testeador de Software

GERENCIA DE INFORMÁTICA Y TECNOLOGÍA ELECTORAL

Jr. Washington 1894, Lima 8, Lima - Perú

Teléfono: (511) 417 0630 Anexo 9074

www.onpe.gob.pe



ADMINISTRACIÓN

R

Registro Nacional

1900.0004

Certificado

13-0001-0004



Certificación Internacional en Eficiencia y Sostenibilidad. Promovemos el respeto y cuidado de los recursos naturales.

Formato de Solicitud de Pase a Control de Calidad

	FORMATO	Código:	FM30-GITE/TI
		Versión:	01
	PASE A CONTROL DE CALIDAD	Fecha de aprobación:	23/06/2017
		Página:	1 de 4

CODIGO DEL PROYECTO	:	SG-415-2015-SGPEL-GITE/ONPE	Nº :	PASCC-046-415
NOMBRE DEL PROYECTO	:	Mantenimiento al Sistema de Gestión Documental		
VERSIÓN	:	3.0		
FECHA	:	08/08/2018	HORA :	16:40 hrs.
LUGAR	:	ONPE- Jr. Washington 1894 – Primer piso		
PARTICIPANTES	:	Emilio Rojas Soria	Coordinador de Proyectos de Desarrollo de Software	
	:	Williams B. Vargas Mamani	Jefe de Control de Calidad de Software	
ASUNTO	:	Entrega del Sistema de Gestión Documental		
LISTA DE ENTREGABLES	:	1. sgd.war		

1. REQUISITOS

1.1. Los requisitos mínimos necesarios de la PC cliente son:

- Windows XP o superior.
- Intel Core Duo CPU 2.00 GHz o superior.
- Memoria RAM de 3.00 GB o superior.
- Navegador Web (Mozilla Firefox v35.0 o superior, Chrome v43.0 o superior, Internet Explorer 11 o superior).
- Borrar la caché de los exploradores Web.
- El usuario debe contar con certificado digital.

1.2. Los prerrequisitos para el ambiente de pruebas son:

- Para la versión de Convenios en los motores de BD el ambiente debe estar con la versión 2.4 de SGD.
- Para la versión de ONPE el ambiente debe estar con la versión 2.4 de SGD.
- Contar con las bases de datos de pruebas de convenios en: ORACLE, SQLSERVER y POSTGRESQL; asimismo contar con la base de datos ORACLE de pruebas de ONPE.
- Contar con un servidor de aplicaciones Glassfish 4.1, considerando que la carpeta /glassfish/tmp debe estar creada.
- Contar con clientes gestores para las 3 diferentes bases de datos. Para la instalación y configuración de los clientes.
- Es importante que el ambiente de pruebas esté configurado con una conexión segura https.

	FORMATO	Código:	FM30-GITE/TI
		Versión:	01
	PASE A CONTROL DE CALIDAD	Fecha de aprobación:	23/06/2017
		Página:	2 de 4

2. LISTA DE ENTREGABLES

2.1. Entregables

Entregable	Tipo	Origen	Destino	Acción	Fecha
sgd	war	Desarrollo	Repositorio QA	Pruebas Funcionales y No Funcionales	08/08/2018

3. DESCRIPCIÓN DETALLADA DE LA LISTA DE ENTREGABLES

No aplica

4. PROCEDIMIENTO

- 4.1. Desplegar el archivo .war entregado, siguiendo los pasos del apartado "3.4. Instalación del SGD" del "Manual de Instalación y Configuración del Servidor de Aplicaciones Convenio SGD", proporcionado por el equipo de Redes. Para el apartado "3.4.2. Configuración de recursos JDBC" del manual en mención, utilizar de preferencia el método 1.

- 4.2. Verificar los datos de los properties siguiendo los pasos del apartado "3.4. Instalación del SGD" del "Manual de Instalación y Configuración del Servidor de Aplicaciones Convenio SGD" proporcionado por el equipo de Redes.

Modificar el archivo "application.properties":

- Modificar la versión del sistema en el parámetro :
✓ "application.version = 2.4" por "application.version = 3.0"
- Modificar el parámetro de la cache local :
✓ localCacheObjects.version=3.0
- Modificar el parámetro de la versión de los recursos:
✓ resources.version=3.0

Agregar un nuevo parámetro en el archivo "application.properties":

#RUC DE RENIEC

nro_ruc_reniec=4F9EC397232AA5383F585D98C41D93BD

Variable de encriptación de parámetros donde "True" indica que se encriptará los parámetros y "False" que no se encriptará los parámetros.
ENCRYPTAR_PARAMETROS_HTTP = true

- 4.3. Acceder al administrador del servidor de aplicaciones, a la opción: Configurations > server-config > JVM settings > JVM Options, ahí debe existir la variable -Dspring.profiles.active=<NOMBRE_BD>, donde <NOMBRE_BD> tendrá 3 posibles valores (oracle, postgresql o sqlserver). Poner el nombre de la base de datos según se requiera y reiniciar el servidor Glassfish.

	FORMATO	Código:	FM30-GITE/TI
		Versión:	01
	PASE A CONTROL DE CALIDAD	Fecha de aprobación:	23/06/2017
		Página:	3 de 4

4.4. Reiniciar el servidor Glassfish.

4.5. Abrir el navegador web e ingresar la siguiente ruta
http://direccion_ip_servidor_web/sqd/login.do.

5. SEGURIDAD

☒ Empleo de técnicas criptográficas.
☒ Permite que el software se ejecute con todos los derechos al usuario que ha iniciado la sesión.
☐ Permite la ejecución del software solo en máquinas específicas.
☐ Utiliza HTTPS Hypertext Transfer Protocol Secure (Protocolo seguro de transferencia de hipertexto).
☒ Utiliza datos encriptados.
☐ Autenticación por usuario y contraseña asignado mediante el MCASL.
☐ Autenticación por usuario y contraseña asignado mediante sobre lacrado.
☐ Autenticación por una tarjeta magnética.
☐ Regla HASH para evitar la modificación del software.
☒ Registro de ficheros con "logs" de actividad.
☐ Privilegios de conexión al servidor.
☐ Asignación de determinadas funcionalidades a determinados usuarios.
☐ Restricciones de comunicación entre determinados módulos.
☐ Bloqueo por intentos fallidos.
☐ Cantidad de accesos permitidos.
☐ Respaldo de información.
☒ Uso de perfiles de acceso.
☐ Otros: _____

6. CONSIDERACIONES

- > Cada vez que se modifica un archivo .properties, se debe reiniciar el servidor de aplicaciones GlassFish.

	FORMATO	Código:	FM30-GITE/TI
		Versión:	01
	PASE A CONTROL DE CALIDAD	Fecha de aprobación:	23/06/2017
		Página:	4 de 4

- Se recomienda que si se modifica un archivo .properties, se reinicia el servidor de aplicaciones y en la PC Cliente no se reflejan cambios, se debe borrar la caché del navegador Web.
- Si no se cuenta con conexión https segura, añadir a las excepciones de seguridad del navegador Web, la URL del SGD y la URL del Web Socket Server.
- Las pruebas deben estar enfocadas al Ethical Hacking, visado de documento con DNI Electrónico, la Integridad del documento y las acciones de descargas de los documentos en formato PDF de los usuarios que tienen permiso de descargar los documentos sin marca de agua en su documento original, siendo registrados en la tabla TDTS_AUDITORIA_MARCA_AGUA.

Firmando en señal de conformidad,



 Firmado digitalmente por ROJAS
 SORLA Emilio O. Sorla
 DN: cn=Emilio O. Sorla, o=ONPE, ou=ONPE, c=PE
 Fecha: 2017.06.23 09:35:13 -0500

Emilio O. Rojas Sorla
 Coordinador de Proyectos de Desarrollo
 de Software

Firmado digitalmente por VARGAS
 MAMANI Williams B. Vargas Mamani
 DN: cn=Williams B. Vargas Mamani, o=ONPE, ou=ONPE, c=PE
 Fecha: 2017.06.23 09:35:13 -0500

Williams B. Vargas Mamani
 Jefe de Control de Calidad de
 Software

Informe de Conformidad de Control de Calidad

	FORMATO	Código:	FM08-GITE/TI
	INFORME DE CONFORMIDAD DE CONTROL DE CALIDAD	Versión:	00
		Página:	1 de 1

PROYECTO	SG-415-2015-SGPOL-GITE/ONPE	Nº	IC-055-415
-----------------	-----------------------------	-----------	------------

LUGAR	: ONPE - Jr. Washington 1894 – Oficina 304		
FECHA	: 22/09/2018	HORA :	09:30 hrs
PARTICIPANTES	: Williams B. Vargas Mamani - Jefe de Control de Calidad de Software. Emilio Oswaldo Rojas Soria - Coordinador de Proyectos de Desarrollo de Software		
ASUNTO	: Mantenimiento al Sistema de Gestión Documental V3.0 sin encriptación		
REFERENCIA	: APCC-032-415_21.09.2018 19:35 hrs		
SISTEMA O PRODUCTO SOFTWARE	: Mantenimiento al Sistema de Gestión Documental		
VERSIÓN	: 3.0		
LISTA DE ENTREGABLES	: sgd.war		

DETALLE DE CONFORMIDAD

Se da conformidad a la actualización APCC-035-415_21.09.2018 del Mantenimiento al Sistema de Gestión Documental V. 3.0 sin encriptación según las indicaciones que menciona el mismo, con las siguientes sugerencias:

- Se sugiere optimizar la referencia a la ruta a almacenamiento de documentos del SGD, si bien no es relevante ni afecta a la funcionalidad, por mejores practicas evite de mostrar error en depuración en el navegador web Google Chrome.
- Se sugiere algún tipo de advertencia que indique que se debe de Ingresar los datos de la persona jurídica durante su registro manual con cuidado porque se replicará en todo el sistema.
- Se sugiere en el momento de crear un empleado con solo apellido materno, este se debiera componerse con la primera letra del nombre y el apellido que está disponible, manteniendo la opción de editar para casos que así lo requieran.
- Se sugiere optimizar la opción de "Seguimiento de Emitidos" en el módulo de consultas, porque afecta al rendimiento.
- En la sección de "Buscar Documento en Referencias", La opción "TODOS" en el combo desplegable es específico en el tipo de búsqueda a realizar, por lo que se sugiere cambiarlo por alguna alternativa como por ejemplo "SELECCIONE DOCUMENTO" que no implique una búsqueda total.

Los archivos de la conformidad se encuentran en la siguiente ruta:

[\\nile-proyectos\PROYECTOS_ONPE\SG-415-2015\03_Conformidades\IC-055-415_22.09.2018](\\nile-proyectos\PROYECTOS_ONPE\SG-415-2015\03_Conformidades\IC-055-415_22.09.2018)

En señal de conformidad se firma el presente documento.

ENTREGADO POR
Williams B. Vargas Mamani
Jefe de Control de Calidad de Software

RECIBIDO POR
Emilio Oswaldo Rojas Soria
Coordinador de Proyectos de Desarrollo de Software

ANEXO 3 – PASE A PRODUCCIÓN

Solicitud de Pase a Producción del Mantenimiento al Sistema de Gestión Documental

Elementos enviados - JCalixto@onpe.gob.pe - Outlook

Reunión, Reenviar, Más, Pasos rápidos, Mover, Reglas, OneNote, No leído/Leído, Categorizar, Seguimiento, Buscar personas, Libreta de direcciones, Filtrar correo electrónico, Buscar, Completar

Responder, Responder a todos, Reenviar

Lunes 24/09/2018 05:26 p.m.

Juan C. Calixto Salazar
RV: [SGD] PASPRO-029-415

Para: DespliegueSGD; Percy E. Mallqui Flores

CC: Lider J. Cotrina Castaneda; Williams Cutipa Chambi; Christian D. Gomez Aguila; Emilio Rojas Soria; Kenny A. Francia Augusto; Frank J. Guzman Castillo; Ronnier Atayauri Calderon; Roxana Z. Cerda Alvarez

Mensaje, PASPRO-029-415[F][F][F].pdf (214 KB), IC-055-415[F][F].pdf (175 KB)

Estimados Percy Buenas tardes,

Por favor su apoyo con la ejecución del **Mantenimiento al Sistema de Gestión Documental**.
Se adjunta los siguientes formatos:

- ✓ Pase a producción (PASPRO-029-415[F][F][F].pdf), el cual se regularizará con las firmas faltantes.
- ✓ Informe de Conformidad de Control de Calidad.

Atentamente,

De: Lider J. Cotrina Castaneda
Enviado el: lunes, 24 de septiembre de 2018 05:16 p.m.
Para: Roxana Z. Cerda Alvarez <rcerda@onpe.gob.pe>
CC: Emilio Rojas Soria <ERojasS@onpe.gob.pe>; Juan C. Calixto Salazar <jcalixto@onpe.gob.pe>
Asunto: RE: [SGD] PASPRO-029-415

De: Roxana Z. Cerda Alvarez
Enviado el: lunes, 24 de septiembre de 2018 02:05 p.m.
Para: Lider J. Cotrina Castaneda <LCotrina@onpe.gob.pe>
CC: Emilio Rojas Soria <ERojasS@onpe.gob.pe>; Juan C. Calixto Salazar <jcalixto@onpe.gob.pe>
Asunto: RV: [SGD] PASPRO-029-415
Importancia: Alta

Juan C. Calixto Salazar
H

No se puede iniciar sesión en: SharePoint. Haga clic aquí para iniciar sesión.

Formato de Solicitud de Pase a Producción

 ONPE ORGANISMO NACIONAL DE PROCESOS ELECTORALES	FORMATO		Código:	FM12-GITE/TI
			Versión:	01
	PASE A PRODUCCIÓN DE UN PRODUCTO SOFTWARE		Página:	1 de 3

N° :	029-415
-------------	----------------

SG-415-2015-SGPEL-GITE/ONPE	PASPRO-029-415
Mantenimiento al Sistema de Gestión Documental	

LUGAR	: ONPE – Jr. Washington 1894 – Piso 1		
FECHA	: 24/09/2018	HORA	: 12:40 hrs.
PARTICIPANTES	Christian Gomez Aguila Sub Gerente de Proyectos Electorales Líder Cotrina Castañeda Sub Gerente de Infraestructura y Seguridad Tecnológica Santos Gonzalez Toranzo Sub Gerente de Innovación, Investigación y Desarrollo Williams Vargas Mamani Jefe de Control de Calidad de Software Emilio Rojas Soria Coordinador de Proyectos de Desarrollo de Software Operador Asignado		
ASUNTO	: Mantenimiento al Sistema de Gestión Documental		
REFERENCIA	: Informe de Conformidad de Control de Calidad N° 055-415		

- REQUISITOS**
 - Servidor de Aplicaciones de Producción.
- LISTA DE ENTREGABLES**
 - Entregables**

ENTREGABLE	TIPO	ORIGEN	DESTINO	ACCIÓN	FECHA
sgd.war	war	 Conformidades/IC-055-415_22.09.2018	Producción	Producción	24/09/2018
- DESCRIPCION DETALLADA DEL (LOS) ENTREGABLE(S)**

✓ sgd.war
- INSTRUCCIONES DE INSTALACIÓN**
 - Desplegar el archivo .war entregado, siguiendo los pasos del apartado "3.4. Instalación del SGD" del "Manual de Instalación y Configuración del Servidor de Aplicaciones Convenio SGD",

	FORMATO	Código:	FM12-GITE/TI
	PASE A PRODUCCIÓN DE UN PRODUCTO SOFTWARE	Versión:	01
		Página:	2 de 3

proporcionado por el equipo de Redes. Para el apartado "3.4.2. Configuración de recursos JDBC" del manual en mención, utilizar de preferencia el método 1.

- 4.2. Verificar los datos de los properties siguiendo los pasos del apartado "3.4. Instalación del SGD" del "Manual de Instalación y Configuración del Servidor de Aplicaciones Convenio SGD" proporcionado por el equipo de Redes.

Modificar el archivo "**application.properties**":

- Modificar el parámetro de la cache local :
✓ `localCacheObjects.version=3.3`
- Modificar el parámetro de la versión de los recursos:
✓ `resources.version=3.3`
- Modificar variable de encriptación de parámetros:
✓ `ENCRIPtar_PARAMETROS_HTTP = true`

- 4.3. Acceder al administrador del servidor de aplicaciones, a la opción: Configurations > server-config > JVM settings > JVM Options, ahí debe existir la variable - `Dspring.profiles.active=<NOMBRE_BD>`, donde `<NOMBRE_BD>` tendrá 3 posibles valores (oracle, postgresql o sqlserver). Poner el nombre de la base de datos según se requiera y reiniciar el servidor Glassfish.

- 4.4. Reiniciar el servidor Glassfish.

- 4.5. Abrir el navegador web e ingresar la siguiente ruta
http://direccion_ip_servidor_web/sqd/login.do.

5. CONSIDERACIONES

- Cada vez que se modifica un archivo .properties, se debe reiniciar el servidor de aplicaciones GlassFish.
- En el caso que en la PC Cliente no se reflejen los cambios, se deberá borrar la caché del navegador Web.
- Si no se cuenta con conexión https segura, añadir a las excepciones de seguridad del navegador Web, la URL del SGD y la URL del Web Socket Server.

En señal de conformidad se firma el presente documento en original y copia.