POSITIVA Compañía de Seguros	**PROCESO:** **GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**	**Código:**	EST_2_2_1_FR03
		Versión:	1
		Fecha:	2018-06-22
	FORMATO **LISTA DE CHEQUEO SEGURIDAD APLICACIONES (OWASP)**		

Aprobó: **Alexander Ruíz Ceballos** Jefe Oficina de Gestión Integral de Riesgos	**Revisó:** **Edwin Mejía Morales** Jefe de Oficina de TI	Elaboró: **Ramiro A. Delvasto** Profesional Especializado Oficina de Gestión Integral de Riesgos **Jesús Alfredo Vargas** Profesional Especializado Oficina de TI

Riesgo	Controles	Validación SI/NO/NA	Evidencia	Observaciones
SQL Injeccion	Utiliza API segura (Validar contra que o como se valida la seguridad) Se debe migrar y utilizar una herramientas de Mapeo Relacional de Objetos (https://www.owasp.org/index.php/Testing_for_ORM_Injection_(OTG-INPVAL-007). Nota: Incluso cuando se parametrizan, los procedimientos almacenados pueden introducir una inyección SQL si el procedimiento PL/SQL o T-SQL concatena consultas y datos, o se ejecutan parámetros utilizando EXECUTE IMMEDIATE o exec().			
	Uso de LIMIT y otros controles SQL para evitar divulgación de registros			
Violación de Autenticación	Uso de múltiples factores de autenticación (Comprobación doble como mínimo)			
	Se hace comprobación de contraseñas débiles			
	Se tiene establecida la longitud y complejidad de la contraseña (Mínimo 8 caracteres, alfanuméricos y siguiendo la política de positiva de control de acceso, la cual puede ser revisada en documento llamado APO 12 4 1 MA01 CONTROL DE ACCESO.pdf encontrado en simple)			
	Se cuenta con conteo de intentos fallido para el bloqueo del usuario (3 intentos)			
Exposición de datos confidenciales	En aplicación se identifican los datos sensibles. No almacene datos sensibles innecesariamente. Descártelos tan pronto como sea posible o utilice un sistema de tokenizacion que cumpla con PCI DSS. Los datos que no se almacenan no pueden ser robados. Remitirse al documento EST_2_2_MA02 Políticas Procedimientos Protección Datos Personales, dato sensible así: aquellos que revelen afiliaciones sindicales, el origen racial o étnico, la orientación política, las convicciones religiosas, morales o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. Para efectos de la Compañía, será Dato Sensible todo aquel que se encuentre relacionado con patologías reconocidas, calificación de origen o pérdida de capacidad laboral de eventos, solicitud y autorización de prestaciones asistenciales, historias clínicas.			
	Los datos almacenados están cifrados			
	Se tiene deshabilitado el almacenamiento en cache de las respuestas con datos confidenciales			
Entidades Externa XML (XXE)	Los procesadores y bibliotecas XML que usa la aplicación están actualizados			
	Esta implementado la validación y filtrado de listas blancas del lado del servidor para prevenir datos hostiles de documentos o encabezado XML			
	Se cuenta con puertas de enlace de seguridad API o firewall de aplicaciones web (WAF)			
Acceso no autorizado	Registro de errores de control de acceso, administradores de alertas (fallas repetidas)			
	Los tokens se invalidan en el servidor después de cerrada la sesión			
Configuración incorrecta de seguridad	Elimina las configuraciones por defecto (características y frameworks) que no son utilizados			
	La aplicación debe tener una arquitectura segmentada que proporcione una separación efectiva y segura entre componentes y acceso a terceros, contenedores o grupos de seguridad en la nube (ACLs).			
Cross-Site Scripting (XXS)	Tiene aplicada un a PSC (política de seguridad de contenido)			
	Aplica frameworks para controlar las entrada de datos de los usuarios			
Deserialización insegura	Se controlan los objetos serializados de fuentes no confiables. Durante la deserialización y antes de la creación del objeto, exija el cumplimiento estricto de verificaciones de tipo de dato, ya que el código normalmente espera un conjunto de clases definibles. Se ha demostrado que se puede pasar por alto esta técnica, por lo que no es aconsejable confiar sólo en ella.			
	Se aplican comprobaciones de integridad a través de firmas digitales			
	se restringe o monitorea la conectividad de red entrante y saliente desde los contenedores o servidores			
Vulnerabilidades	Se eliminan dependencias no utilizadas, características, componentes y archivos innecesarios			
	Uso de componente y librerías de fuentes confiables. Obtener componentes únicamente de orígenes oficiales utilizando canales seguros. Utilizar preferentemente paquetes firmados con el fin de reducir las probabilidades de uso de versiones manipuladas maliciosamente			
	Plan de actualizaciones de bibliotecas utilizadas			
Monitoreo y registro	Se tienen activos los logs de auditoria de acceso a al aplicación			
	Los logs se generan en un formato entendible y fácil de auditar			
	Las transacciones de alto valor tienen seguimiento a través de los logs de auditoria			
	Se tienen establecido el plan de restauración de la aplicación ante un incidente.			
Fuente:	https://owasp.org			

CONTROL DE CAMBIOS

No.	Descrpción del Cambio	Fecha del cambio	Quien aprueba el cambio (cargo)	Versión Anterior
1	Se crea el formato	22/06/2018	Jefe Oficina Gestión Integral de Riesgos	N/A