INFORME FINAL EJECUTIVO ACTIVIDADES COLJUEGOS

SEPTIEMBRE 2023

Contenido

1. Objetivo 2
2. Alcance 2
3. Detalle actividades y estado 3

1. Objetivo

Informar el cierre final de las actividades realizadas por Password Consulting S.A.S de acuerdo con el contrato 113 de 2023 con Coljuegos.

2. Alcance

El presente informe ejecutivo contempla las actividades correspondientes para el pago del 70% y aquellas que han sido finalizadas de acuerdo con el contrato 113 de 2023 con la entidad Coljuegos y Password Consulting S.A.S:

1. Instructivo de clasificación y etiquetado de activos de información.
2. Documento que contenga la metodología utilizada, resumen de actividades, principales hallazgo s, conclusiones y recomendaciones.
3. Informe de los resultados de pruebas presenciales y no presenciales que contengan como mínimo:
    - Explicación de la metodología empleada por las diferentes técnicas
    - Resultado de ejecución de las pruebas
    - Evidencias fotográficas en caso que aplique
    - Vulnerabilidades encontradas y riesgos encontrados a partir de las mismas
    - Documento plan de acción para la mitigación de los riesgos encontrados
4. Informe de los resultados de las pruebas de Fake mailing
5. Gestión de riesgos de seguridad de la información:
    - Documento con la metodología de la gestión de riesgos.
    - Matriz de valoración riesgos de seguridad de la información
    - Documento con el plan de tratamiento de riesgos
6. Elaborar un plan de remediación conforme a los resultados de las actividades
7. Documento de recomendaciones basado en los resultados.
8. Procedimiento para la gestión de vulnerabilidades técnicas donde se indique la metodología, tipos de pruebas, frecuencia de los escaneos a la infraestructura tecnológica de la entidad para mantener esta ejecución en el tiempo.

De igual forma se incluyen las obligaciones especificas que hacen parte del anexo técnico y cumplidas en el 70% del contrato, igualmente se mantiene el informe de las actividades correspondientes al 30% inicial del contrato para un total del 100%.

3. Detalle actividades y estado

A continuación, se describen las actividades ejecutadas para el contrato 113 de 2023, su estado y entregable correspondientes al 30%

ACTIVIDAD CORRESPONDIENTE AL 30%	OBLIGACIÓN ESPECIFICA	FECHA ACTIVIDAD EJECUTADA	ESTADO	ACTIVIDADES EJECUTADAS	NOMBRE DE LA EVIDENCIA
Plan de gestión del proyecto	NA	3/05/2023	Realizada	Reunion de Inicio del proyecto, presentación de cronograma y los riesgos del proyecto, Se remitió el plan del proyecto el 23/05/203	**Plan de Proyecto - Coljuegos (05.23)** https://docs.google.com/document/d/1NjlO24UZNCYXYJmFva6oF6mGkIgm6SGs/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true
Metodología de Ethical Hacking	Testear los sistemas operativos, su configuración, puertos activos y servicios en comparación con la documentación del sistema.	9/06/2023	Realizada	Se documentó la metodología para llevar a cabo las pruebas de vulnerabilidad y ethical hacking (15/05/2023) Fue realizada la socialización de Ethical Hacking Se presentó el plan de pruebas el cual contiene la metodología para ejecutar las pruebas de vulnerabilidad y ethical hacking. (09/06/2023)	**Metodología Ethical Hacking - Coljuegos (05.23)** https://docs.google.com/document/d/1JR3dkFghEnoDl7W9GrEsiIxzxkPK0Zw-/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true
	Realizar análisis de vulnerabilidades en los hosts de la entidad y así mismo realizar re-test de las pruebas de vulnerabilidad				
	Realizar pruebas de integridad a todos los resultados.				
	Realizar pruebas de integridad a todos los resultados.				
	Realizar prueba de intrusión en la red de área local (LAN) tanto alámbrica como inalámbrica y con base en esta determinar el estado actual de la infraestructura tecnológica.				
	Realizar pruebas de Hacking Ético: Buffer-Overflows, descubrimiento de contraseñas a la fuerza, cracking de contraseñas sobre cuentas privilegiadas de Base de Datos, secuestro de sesiones, errores en aplicaciones				

ACTIVIDAD CORRESPONDIENTE AL 30%	OBLIGACIÓN ESPECIFICA	FECHA ACTIVIDAD EJECUTADA	ESTADO	ACTIVIDADES EJECUTADAS	NOMBRE DE LA EVIDENCIA
	o configuraciones débiles.				
	Realizar prueba de penetración en la IPs públicas, definidos en el alcance con el fin de determinar el estado actual de la infraestructura tecnológica y la seguridad de su interconexión.				
	Cumplir y desarrollar las actividades de servicios de seguridad para el fortalecimiento de la ciberseguridad, de conformidad con las condiciones establecidas en el ANEXO 1 “Especificaciones Técnicas”.				
Cronograma de ejecución	NA	23/05/2023	Realizada	Reunion de Inicio del proyecto , presentación de cronograma y los riesgos del proyecto, Se remitió el cronograma del 02/06/2023	**Anexo Nº. 1 – Cronograma Seguridad – Coljuegos (05.23).pdf** https://drive.google.com/file/d/1seFTG58w7eI_hXpBQegHJvAxHUaeMnyy/view?usp=drive_link
Informe de resultados del análisis, evaluación y diagnóstico de la situación actual e Identificación de brechas para cada dominio de ISO/IEC 27001.	Cumplir y desarrollar las actividades de servicios de seguridad para el fortalecimiento de la ciberseguridad, de conformidad con las condiciones establecidas en el ANEXO 1 “Especificaciones Técnicas”.	18/07/2023	Realizada	Fue realizado a través de sesiones y entrevistas el diagnóstico en la Norma ISO:27001:2022.	**Informe Diagnóstico SGSI - COLJUEGOS (24.07)** https://docs.google.com/presentation/d/1YIo750PmBC9kNb97-r-hwICDRWjpE2dF/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true
				Se realizó informe con resultados y recomendaciones el cual ya se encuentra en el repositorio.	
				Fue socializado informe con Coljuegos, en el cual se indica:	**Cto 113 Coljuegos GAP- ISO 27001 2022 (24.07)** https://docs.google.com/spreadsheets/d/1kCR0op-DXVnSzxZnRF7_wX-z6ySCBdp3/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true
				· Calificación actual	**Presentación Informe Diagnóstico SGSI - COLJUEGOS (24.07)** https://docs.google.com/presentation/d/1YIo750PmBC9kNb97-r-hwICDRWjpE2dF/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true
				· Resultado dominios A5,A6,A7 y A8.	
				· Ruta de trabajo	
				· Recomendaciones	

ACTIVIDAD CORRESPONDIENTE AL 30%	OBLIGACIÓN ESPECIFICA	FECHA ACTIVIDAD EJECUTADA	ESTADO	ACTIVIDADES EJECUTADAS	NOMBRE DE LA EVIDENCIA
				Se encuentra pendiente agendar sesión para atender preguntas sobre el diagnóstico.	
Informe Ejecutivo y técnico de Resultados de vulnerabilidades	Realizar el análisis de vulnerabilidades para determinar las debilidades existentes de los servicios a nivel interno y externo, aplicando como metodología base el marco de referencia OSSTMM (open Source Security Testing Methodology Manual) y la OSCP (Offensive Security Certified Professional). Testear los sistemas operativos, su configuración, puertos activos y servicios en comparación con la documentación del sistema. Realizar análisis de vulnerabilidades en los hosts de la entidad y así mismo realizar re-test de las pruebas de vulnerabilidad Realizar pruebas de integridad a todos los resultados. Elaborar y sustentar un informe de resultado que contenga los hallazgos tras el análisis de vulnerabilidad en la cual se puedan identificar los puntos críticos que deberán ser priorizados. Elaborar plan de recomendaciones, que apoyará la priorización de los hallazgos. Cumplir y desarrollar las actividades de servicios de seguridad para el fortalecimiento	13/07/2023	Realizada	Se elaboró el informe de las pruebas de vulnerabilidad y se presentó ante la Entidad de forma presencial el día 13/07/2023	**Informe Análisis de Vulnerabilidades - Coljuegos v2** https://drive.google.com/file/d/10rM3aOmzGtnwGwhHMmMcbh-t0UsgYTcp/view?usp=drive_link **Presentación Ejecutiva Resultados Pruebas Vulnerabilidad - Coljuegos v1** https://drive.google.com/file/d/14HYF1aQgrfxklHQrrj6gXmbYSRuKUYaS/view?usp=drive_link **Anexo 2. Informe técnico de vulnerabilidades Infraestructura** https://docs.google.com/spreadsheets/d/1kHHBRaIHT_yYiyGueVhcCg-DWYakdISW/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true **Anexo 3. Informe técnico de vulnerabilidades Web** https://docs.google.com/spreadsheets/d/12D70qg8rQL_y63UrHjCSOqywCKqDBD05/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true

ACTIVIDAD CORRESPONDIENTE AL 30%	OBLIGACIÓN ESPECIFICA	FECHA ACTIVIDAD EJECUTADA	ESTADO	ACTIVIDADES EJECUTADAS	NOMBRE DE LA EVIDENCIA
	de la ciberseguridad, de conformidad con las condiciones establecidas en el ANEXO 1 “Especificaciones Técnicas”.				

A continuación, se describen las actividades ejecutadas para el contrato 113 de 2023, su estado y entregable correspondientes al 70%

ACTIVIDAD CORRESPONDIENTE AL 70%	OBLIGACIÓN ESPECIFICA	FECHA ACTIVIDAD EJECUTADA	ESTADO	ACTIVIDADES EJECUTADAS	NOMBRE DE LA EVIDENCIA
Instructivo de clasificación y etiquetado de activos de información.	Cumplir y desarrollar las actividades de servicios de seguridad para el fortalecimiento de la ciberseguridad, de conformidad con las condiciones establecidas en el ANEXO 1 “Especificaciones Técnicas”.	12/06/2023	Realizado	Se construyo el instructivo de etiquetado y fue socializado al área de planeación al área de la OTIC el cual fue aprobado	Coljuegos Instructivo Etiquetado Información (06.23) https://drive.google.com/drive/folders/1xWsS-A__qp-6H8G4IlXPhPTaCyoEeiDc
Documento que contenga la metodología utilizada, resumen de actividades, principales hallazgos, conclusiones y recomendaciones.	Realizar el análisis de vulnerabilidades para determinar las debilidades existentes de los servicios a nivel interno y externo, aplicando como metodología base el marco de referencia OSSTMM (open Source Security Testing Methodology Manual) y la OSCP (Offensive Security Certified Professional).	11/05/2023	Realizado	Se realizo el documento y se socializo la metodología con la OTIC	Metodología Identificación de Riesgos - Ajustes Password (07.23).docx https://docs.google.com/document/d/1ceNvuYauQeOqQoybPE_OAafcQGVEy5o-/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true

ACTIVIDAD CORRESPONDIENTE AL 70%	OBLIGACIÓN ESPECIFICA	FECHA ACTIVIDAD EJECUTADA	ESTADO	ACTIVIDADES EJECUTADAS	NOMBRE DE LA EVIDENCIA
Informe de los resultados de pruebas presenciales y no presenciales que contengan como mínimo: **• Explicación de la metodología empleada por las diferentes técnicas** **• Resultado de ejecución de las pruebas** **• Evidencias fotográficas en caso que aplique** **• Vulnerabilidades encontradas y riesgos encontrados a partir de las mismas** **• Documento plan de acción para la mitigación de los riesgos encontrados**	Testear los sistemas operativos, su configuración, puertos activos y servicios en comparación con la documentación del sistema. Realizar pruebas de integridad a todos los resultados Elaborar y sustentar un informe de resultado que contenga los hallazgos tras el análisis de vulnerabilidad en la cual se puedan identificar los puntos críticos que deberán ser priorizados. Elaborar plan de recomendaciones , que apoyará la priorización de los hallazgos. Realizar análisis de vulnerabilidades en los hosts de la entidad y así mismo realizar re-test de las pruebas de vulnerabilidad.	24/07/2023	Realizado	Se elaboro el documento y se socializo el informe de análisis d vulnerabilidades	Informe Análisis de Vulnerabilidades - Coljuegos v2.pdf https://drive.google.com/file/d/1YRcd0fjjf768F3n1ezy6EPVRRKT4FZC0/view?usp=drive_link
Informe de los resultados de las pruebas de Fake mailing	Realizar pruebas de Hacking Ético: Buffer-Overflows, descubrimiento de contraseñas a la fuerza, cracking de contraseñas sobre cuentas privilegiadas de Base de Datos, secuestro de sesiones, errores	26/09/2023	Realizado	Se elaboró el documento y se socializó el informe de análisis d vulnerabilidades	Informe de ingeniería social Fake Mail - Coljuegos (09.2023) https://docs.google.com/document/d/1cnXGpeI9Q39_7gkSrBbl0eGLh0oXrNp5/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true

ACTIVIDAD CORRESPONDIENTE AL 70%	OBLIGACIÓN ESPECIFICA	FECHA ACTIVIDAD EJECUTADA	ESTADO	ACTIVIDADES EJECUTADAS	NOMBRE DE LA EVIDENCIA
	en aplicaciones o configuraciones débiles Elaborar plan de recomendaciones, que apoyará la priorización de los hallazgos.				
Gestión de riesgos de seguridad de la información: **• Documento con la metodología de la gestión de riesgos.** **• Matriz de valoración riesgos de seguridad de la información** **• Documento con el plan de tratamiento de riesgos**	Cumplir y desarrollar las actividades de servicios de seguridad para el fortalecimiento de la ciberseguridad, de conformidad con las condiciones establecidas en el ANEXO 1 "Especificaciones Técnicas".	10/08/2023	Realizado	Se elaboró el documento y se socializó el informe de análisis de vulnerabilidades	IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS.docx https://docs.google.com/document/d/11fevVMuOciZqlQQ69E7DIGtIX99fz74g/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true
Elaborar un plan de remediación conforme a los resultados de las actividades	Elaborar y sustentar un informe de resultado que contenga los hallazgos tras el análisis de vulnerabilidad en la cual se puedan identificar los puntos críticos que deberán ser priorizados.	24/08/2023 29/09/2023	Realizado Realizado	Se elaboró el documento y se socializó el informe	Informes Pruebas de Vulnerabilidad y EH.zip https://drive.google.com/file/d/1BszExwZ0v1uZnBcpKUVp_RQ09lsTaiFa/view?usp=drive_link Coljuegos- Plan Acción Tratamiento Riesgo (08.23).docx https://docs.google.com/document/d/13VlZHxk3lrFGZPy_DkiO7KoURU5WUccU/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true Informe-Evaluacion-FW.docx https://docs.google.com/document/d/1_85untIR_AgAppfmfI79oBCys1XY934z/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true
Documento de recomendaciones basado en los resultados.	Elaborar plan de recomendaciones, que apoyará la priorización de los hallazgos.	24/08/2023 29/09/2023	Realizado Realizado	Se elaboró el documento y se socializó el informe Se elaboró el documento	Procedimiento de Gestión Técnica de Vulnerabilidades (1) https://drive.google.com/file/d/1AaeltCwfcvq5XKE4ZLQFkJbV0e6QzxlX/view?usp=drive_link Informe-Evaluacion-FW.docx https://docs.google.com/document/d/1_85untIR_AgAppfmfI79oBCys1XY934z/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true

ACTIVIDAD CORRESPONDIENTE AL 70%	OBLIGACIÓN ESPECIFICA	FECHA ACTIVIDAD EJECUTADA	ESTADO	ACTIVIDADES EJECUTADAS	NOMBRE DE LA EVIDENCIA
		28/09/2023	Realizado	Se elaboró el documento	Informe de ingeniería social OSINT - Coljuegos (09.2023).docx https://docs.google.com/document/d/1QwOb43pqKx-AvnsQCoFPEZG9RnQsLlWn/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true
Procedimiento para la gestión de vulnerabilidades técnicas donde se indique la metodología, tipos de pruebas, frecuencia de los escaneos a la infraestructura tecnológica de la entidad para mantener esta ejecución en el tiempo	Realizar el análisis de vulnerabilidades para determinar las debilidades existentes de los servicios a nivel interno y externo, aplicando como metodología base el marco de referencia OSSTMM (open Source Security Testing Methodology Manual) y la OSCP (Offensive Security Certified Professional).	24/08/2023	Realizado	Se elaboró el documento y se socializó el informe	Procedimiento de Gestión Técnica de Vulnerabilidades (1) https://drive.google.com/file/d/1AaeltCwfcvq5XKE4ZLQFkJbV0e6QzxlX/view?usp=drive_link
Cumplir con 60 horas de transferencia de conocimiento de los temas abordados en el objeto contractual, de acuerdo a la oferta presentada.	Cumplir con 60 horas de transferencia de conocimiento de los temas abordados en el objeto contractual, de acuerdo a la oferta presentada.	11/09/2023 – 12/09/2023	Vaucher	Se hizo uso de las 3 horas adicionales de capacitación.	Plan de Capacitación Coljuegos (08.23).docx https://docs.google.com/document/d/1cFns-RqwHUSSQojMghZdGsptJruXjPvf/edit?usp=drive_link&ouid=104248612214889873522&rtpof=true&sd=true
Vaucher	Cumplir con 60 horas de transferencia de conocimiento de los temas abordados en el objeto contractual, de acuerdo a la oferta Presentada Retest de vulnerabilidades (Ejecutar retest teniendo en cuenta las pruebas iniciales	29/09/2023	Vaucher	Se genera el compromiso en virtud a la necesidad del cliente de contar con tiempo suficiente para efectuar las remediaciones y para hacer uso de las horas pendientes	

ACTIVIDAD CORRESPONDIENTE AL 70%	OBLIGACIÓN ESPECIFICA	FECHA ACTIVIDAD EJECUTADA	ESTADO	ACTIVIDADES EJECUTADAS	NOMBRE DE LA EVIDENCIA
	de análisis de vulnerabilidad - Elaborar informe de retest - Socializar y enviar el informe final de Retest),				