

Análisis Integral de Riesgos para nuevos productos, proceso, servicios y/o proyectos

Nombre: Herramienta de acompañamiento - Propulsor	Fecha	2021	05	26
		Año	Mes	Día

Unidad de Análisis:

Proceso al que pertenece:

Fomento empresarial

Líderes del proceso:

Luis Miguel Alvarez Venegas

Descripción:

Fundación Coomeva está próxima a realizar la renovación del contrato de arrendamiento de la aplicación propulsor (<https://coomeva.propulsor.com.co>) que se tiene con la empresa I-VOLUCION PROYECTOS PARA EL DESARROLLO SAS. Aplicación a través de la cual se permite que los asociados puedan llevar a cabo la realización de diagnósticos empresariales, agendar sesiones con consultores de su interés, contar en un solo espacio con la oferta del ecosistema de emprendimiento nacional y además realizar seguimiento a su plan de fortalecimiento; y permite a Fundación Coomeva la generación, consulta y descarga de informes.

Metodología: *La elaboración de este informe, se realiza llevando a cabo las actividades de identificación del riesgo, análisis del riesgo y valoración del riesgo.*

En la actividad de identificación del riesgo se lleva a cabo el conocimiento de los detalles de la ejecución de cada una de las actividades que componen el proceso o iniciativa, y se complementa con información de análisis previos, documentación soporte como contratos, procedimientos o instructivos. El objetivo de esta actividad es generar una lista de potenciales eventos de riesgos (no hallazgos) que tienen la capacidad de reducir, retrasar, impedir o impulsar (si se trata de oportunidades) la consecución de los objetivos, poner en riesgo la información del GECC o de los asociados, colaboradores o proveedores e incumplir con las regulaciones de entes externos.

Riesgos Seguridad y privacidad de la Información

No	Riesgo	Causa	Control/Recomendación	Responsable	Nivel de Riesgo	Seguimiento
1.	Fuga de información del asociado	Ausencia o insuficiencia de un proceso que asegure la gestión de vulnerabilidades en la infraestructura que soporta la aplicación Propulsor. (sistemas operativos, servidores de aplicaciones, bases de datos, etc.).	<p>1. Realizar pruebas de vulnerabilidad / pruebas de penetración periódicas, o cada vez que se realice un cambio significativo sobre la infraestructura que soporta el servicio y la aplicación; garantizando el tratamiento oportuno de las debilidades identificadas.</p> <p>2. Incluir en el contrato una cláusula que exija la ejecución periódica del control anteriormente descrito.</p>	<p>Proveedor I- VOLUCION PROYECTOS PARA EL DESARROLLO SAS</p> <p>Jefe Nacional Servicio Desarrollo Empresarial Fun</p>	Alta	
		Ausencia o insuficiencia de un proceso de desarrollo seguro por parte del proveedor.	Adoptar prácticas de desarrollo seguro durante la construcción y mantenimiento de la aplicación Propulsor (análisis de código activo) y las integraciones con Coomeva.	<p>Proveedor I- VOLUCION PROYECTOS PARA EL DESARROLLO SAS</p>	Alta	
		Deficiencia en el proceso de ingreso seguro de los usuarios administradores a la aplicación, debido a que no se tiene implementado un mecanismo de autenticación de doble factor para el ingreso de los mismos a la aplicación.	Se debe adoptar el uso de una aplicación de autenticación (Google Authenticator, Microsoft Authenticator, Authy, etc.) como mecanismo de segundo factor de autenticación.	<p>Proveedor I- VOLUCION PROYECTOS PARA EL DESARROLLO SAS</p>	Alta	

		Deficiencia en el proceso de ingreso seguro de los usuarios administradores a la base de datos, debido a que no se tiene implementado un mecanismo de autenticación fuerte para el ingreso de los usuarios administradores a la misma.	Se debe adoptar un mecanismo de autenticación fuerte, en el cual se asegure el uso de protocolos seguros.	Proveedor I- VOLUCION PROYECTOS PARA EL DESARROLLO SAS	Alta	
		Ausencia o insuficiencia en el control de las operaciones realizadas sobre la base de datos en la cual queda almacenada la información de los usuarios de la aplicación (Nombres, Apellidos, Cédula, e-Mail, Numero celular, etc.).	Se debe asegurar la auditoria, monitoreo y protección de las operaciones realizadas sobre los datos que reposan en la base de datos.	Proveedor I- VOLUCION PROYECTOS PARA EL DESARROLLO SAS	Alta	
		Robo o pérdida de los equipos de cómputo “portátiles” de los colaboradores que participan en el proceso.	Implementar control de cifrado de disco y/o archivos en los equipos de cómputo “portátiles” de los colaboradores que participan en el proceso, haciendo uso de las herramientas de cifrado definidas por el GECC (McAfee Drive Encryption y McAfee File and Removable Media Protection).	Jefe Nacional Servicio Desarrollo Empresarial Fun	Alta	
		Deficiencias en la implementación de controles de seguridad para dispositivos USB/medios extraíbles sobre los equipos de cómputo de los colaboradores que participan en el proceso.	Implementar control de bloqueo de dispositivos USB/medios extraíbles en los equipos de cómputo de los colaboradores que participan en el proceso, haciendo uso de las herramientas definidas por el GECC (McAfee Device Control).	Jefe Nacional Servicio Desarrollo Empresarial Fun	Alta	
2.	Fuga y/o modificación de información del asociado	Deficiencia en el proceso de ingreso seguro de los usuarios a la aplicación, debido a que solo se solicita el identificador de usuario para acceder a la misma.	Se debe adoptar un mecanismo de ingreso seguro, en el cual se le solicite al usuario de la aplicación su identificación de usuario y una contraseña. Se debe tener en cuenta que debido a que se permitirá el registro en la	Proveedor I- VOLUCION PROYECTOS PARA EL DESARROLLO	Extrema	

			aplicación de asociados y no asociados a la cooperativa, se debe solicitar el acompañamiento de arquitectura de soluciones de la GCT&TD, para poder implementar el control requerido.	SAS Jefe Nacional Servicio Desarrollo Empresarial Fun		
3.	Incumplimiento de ley de protección de datos personales (Ley 1581 de 2012)	Deficiencia en la presentación de la finalidad de tratamiento de los datos personales y en el almacenamiento de la autorización dada por el titular para el tratamiento de sus datos personales.	<p>1. Presentar de forma clara cuál es la finalidad de la recolección de datos personales.</p> <p>2. Asegurar que la autorización quede almacenada en la base de datos local de la aplicación y que se incluya la siguiente marca de tiempo e información:</p> <ul style="list-style-type: none"> • Hora del día: Expresada como hora, minutos, segundos (hh: mm: ss), de acuerdo con el estándar internacional de mediciones. • Fecha: Expresada como día, mes y año (dd: mm: aaaa). • Dirección IP: Dirección IP que registra el usuario al momento de otorgar la autorización. • Nombre de la aplicación: Nombre de la aplicación o formulario a través de la cual se recolecta la autorización. • Nombre de la empresa: Nombre de la empresa que recolecta la autorización. 	<p>Jefe Nacional Servicio Desarrollo Empresarial Fun</p> <p>Proveedor I- VOLUCION PROYECTOS PARA EL DESARROLLO SAS</p>	Extrema	
		Ausencia o insuficiencia de un proceso, por parte del proveedor, que asegure la detección y reporte a Fundación Coomeva de cualquier incidente de seguridad y	1. Implementar un proceso que asegure la detección y reporte a Fundación Coomeva de cualquier incidente de seguridad y privacidad de la información a través de los canales	<p>Proveedor I- VOLUCION PROYECTOS PARA EL</p>	Extrema	

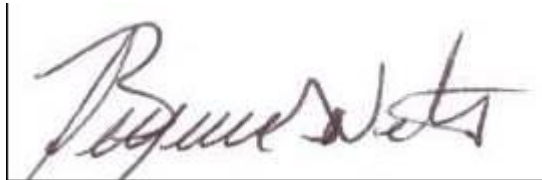
		privacidad de la información que se presente en la infraestructura que soporta la aplicación Propulsor. (sistemas operativos, servidores de aplicaciones, bases de datos, etc.).	<p>definidos, indicando los detalles y acciones adoptadas en relación con la respuesta, contención, solución y documentación del incidente.</p> <p>2. Incluir en el contrato una cláusula que exija el reporte de los incidentes de seguridad y privacidad de la información..</p>	DESARROLLO SAS Jefe Nacional Servicio Desarrollo Empresarial Fun		
4.	Obtención de información	Debilidades en las competencias en materia de seguridad y privacidad de la información por parte de los colaboradores de Fundación Coomeva y del proveedor que participan en el proceso.	Garantizar capacitaciones y sensibilizaciones periódicas para fortalecer competencias en materia de seguridad y privacidad de la información a los colaboradores de Fundación Coomeva y los colaboradores del proveedor, que participan en el proceso (como mínimo una vez al año).	<p>Jefe Nacional Servicio Desarrollo Empresarial Fun</p> <p>Proveedor I-VOLUCION PROYECTOS PARA EL DESARROLLO SAS</p>	Moderada	

Nivel de Riesgo Seguridad y privacidad de la Información

Alta – Se identifican riesgos potenciales que, para poder ser mitigados, se requiere endurecer los controles técnicos y administrativos que actualmente se tienen implementados en el proceso y en la aplicación propulsor; y de esta forma poder proteger la información de los asociados y no asociados que se almacena en la infraestructura del proveedor y en los equipos de cómputo de los colaboradores de Fundación Coomeva.

Conclusiones /Recomendaciones

- Se considera importante que la aplicación propulsor tenga un mecanismo que autentique asociados y no asociados; el cual debe ser revisado y discutido con la UTI.

A handwritten signature in dark ink, appearing to read "Benjamin Nates Medina".

Benjamin Andrés Nates Medina
Coordinador Seguridad Información UCO

Luis Miguel Alvarez Venegas
Jefe Nacional Servicio Desarrollo Empresarial Fun

Copia: Nombre y cargo de las personas a quien se otorgará copia del informe.