FONPRECON Pensiones y Cesantías	MAPA DE RIESGOS SEGURIDAD DE LA INFORMACIÓN -SEGURIDAD DIGITAL Norma Tecnica Colombiana NTC-ISO-IEC 27001	CODIGO: MAP-SGSI-001 VERSIÓN 2 Fecha de aprobación 27/07/2021

Nro.	RIESGO	ACTIVO	TIPO	AMENAZAS	DESCRIPCIÓN DEL RIESGO TIPO	CAUSA / VULNERABILIDAD	CONSECUENCIA	RIESGO INICIAL O INHERENTE		
								CALIFICACIÓN		ZONA DE RIESGO RESIDUAL
								PROBABILIDAD	IMPACTO	
1	Pérdida de Confidencialidad	RECURSO HUMANO	Seguridad de Información	Usuarios mal intencionados o sin conocimientos en seguridad de la información.	Practicas inadecuadas en seguridad de la información por parte los funcionarios públicos de Fonprecon	1. Falta de revisiones periódicas a la política general y/o a políticas específicas de seguridad de la información. 2. Servidores con privilegios inadecuados de acceso a la información, e inadecuado uso de la información.	. Desactualización de politicas de seguridad de la información . Incumplimiento de politicas de seguridad de la información . Pérdida imagen institucional . Sanciones disciplinarias o penales	Improblable	Moderado	Moderado
2	Pérdida de Integridad	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Seguridad de Información	Incendio, inundación, polvo, funcionarios con acceso a Datacenter, proveedores tecnológicos, códigos maliciosos (Spyware, Troyanos, Virus, Gusanos) Información inexacta o adulterada	Daño de información o en las instalaciones de procesamiento de datos (Datacenter)	1. Ausencia de planes de emergencia y pruebas al mismo. 2. Ausencia de redes contra incendio. 3. Falta de controles de acceso físico o deficiencia de los mismos. 4. Privilegios inadecuados de acceso para modificar información producida en los diferentes procesos.	.Interrupción completa de los servicios ofrecidos por Fonprecon . Información inexacta .Pérdidas económicas .Pérdida imagen institucional .Sanciones disciplinarias y penales	Improblable	Mayor	Alto
3	Perdida de Integridad	HARDWARE SOFTWARE Y SERVICIOS	Seguridad de Información	Usuarios mal intencionados, códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), software con vulnerabilidades	Instalación y uso de software con vulnerabilidades conocidas en los sistemas operativos de los equipos de cómputo y servidores	1. Ausencia de políticas y controles restrictivos para la instalación de software no autorizado 2. Uso e instalación de software con vulnerabilidades 3. Perfiles y privilegios no asignados	Interrupción de las operaciones y/o afectación en la prestación del servicio	Probable	Mayor	Extremo
4	Pérdida de Confidencialidad	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Seguridad de Información	Códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), usuarios sin conocimiento de las políticas de seguridad de la información Servidores públicos que utilizan indebidamente las redes informáticas	Infección de equipos informáticos (equipos de cómputo, servidores, equipos de comunicaciones, seguridad, dispositivos móviles) ocasionado por la pérdida de la confidencialidad.	1. Base de datos de antivirus desactualizada. 2. Uso de medios removibles. 3. Uso de las redes para actividades diferentes a las laborales.	Posibles fallos de seguridad o vulnerabilidades en los equipos informáticos y/o perdida de información sensible y confidencial de Fonprecon	Posible	Moderado	Alto
5	Pérdida de Disponibilidad	INFORMACIÓN RECURSO HUMANO	Seguridad de Información	Proveedores externos, Atacantes, Códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), servicios de suministro, amenazas naturales (terremotos, incendios, inundaciones, polvo)	Pérdida de la información digital dada en custodia al proveedor de Backup's (daño, robo, pérdida)	1. Manipulación, transporte y almacenamiento inadecuado a las cintas de backups. 2. Ausencia de pruebas regulares a las copias de respaldo.	Perdida de la información y posibles ataques a la integridad de los datos.	Improblable	Menor	Bajo
6	Pérdida de Disponibilidad	INFORMACIÓN RECURSO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Seguridad de Información	Administrador de servidores sin conocimiento de las políticas de seguridad de la información, Códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), Atacantes Utilizacion indebida de dispositivos extraibles para guardar información que reposa en los equipos de cómputo, o carga de energia de dispositivos móviles en las entradas USB.	Pérdida de la información generada por las actividades propias de la gestión del proceso	1. Ausencia de medidas para evitar la pérdida de datos, por ejemplo copias de respaldo. 2. Falta de pruebas regulares a las copias de respaldo. 3. Ausencia de manuales para la administración de las herramientas de aplicaciones. 4. Servideres públicos sin conciencia o conocimiento de los posibles daños o pérdida de información.	Perdida de confidencialidad y disponibilidad de la información para los usuarios internos y externos.	Improblable	Mayor	Alto
7	Pérdida de Confidencialidad	INFORMACIÓN RECURSO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Seguridad de Información	Activos de información, usuarios sin conocimiento de las políticas de seguridad de la información	Uso inadecuado de los activos de información (tipo servicios, hardware, software, RECURSO HUMANO, información física y digital)	1. Ausencia de políticas y controles para la gestión adecuada de los activos de información. 2. Falta de sensibilización en el uso adecuado de los activos de información.	Perdida, robo o mala utilización de la información.	Posible	Moderado	Alto

FONPRECON Pensiones y Cesantías	MAPA DE RIESGOS SEGURIDAD DE LA INFORMACIÓN -SEGURIDAD DIGITAL Norma Tecnica Colombiana NTC-ISO-IEC 27001	CODIGO: MAP-SGSI-001 VERSIÓN 2 Fecha de aprobación 27/07/2021

Nro.	RIESGO	ACTIVO	TIPO	AMENAZAS	DESCRIPCIÓN DEL RIESGO TIPO	CAUSA / VULNERABILIDAD	CONSECUENCIA	RIESGO INICIAL O INHERENTE		
								CALIFICACIÓN		ZONA DE RIESGO RESIDUAL
								PROBABILIDAD	IMPACTO	
8	Pérdida de Integridad	RECURSO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Seguridad de Información	Códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), administradores de tecnología sin conocimientos técnicos de seguridad de la información.	Ataques informáticos internos/externos a la infraestructura tecnológica (páginas web, software misional, hardware, aplicaciones, equipos de comunicación, equipos de seguridad, red interna)	1. Vulnerabilidades técnicas sin conocer, uso de software desactualizado 2. Falta de sensibilización del personal sobre ataques cibernéticos	Perdida de la continuidad del negocio, servicios afectados para los usuarios internos y externos. Afectación a toda la Entidad	Posible	Moderado	Alto
9	Pérdida de Confidencialidad	INFORMACIÓN RECURSO HUMANO	Seguridad de Información	Usuarios sin conocimiento de las políticas de seguridad de la información y sin sensibilización.	Gestión y uso inadecuado de las contraseñas	1. Ausencia de políticas para la gestión y uso de contraseñas 2. Falta de sensibilización y capacitación en el uso de contraseñas	Incumplimiento de las políticas de seguridad de la información	Probable	Mayor	Extremo
10	Pérdida de Confidencialidad	RECURSO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Seguridad de Información	Red sin protección, usuarios mal intencionados, Códigos maliciosos (Spyware, Troyanos, Virus, Gusanos)	Acceso no autorizado a las redes de la entidad (interna y externa)	1. Ausencia de controles que protejan la información transferida y las instalaciones de procesamiento de información de soporte	Perdida de imagen ante los usuarios y perdida de confidencialidad de la información	Improblable	Menor	Bajo
11	Pérdida de Confidencialidad	RECURSO HUMANO	Seguridad de Información	Funcionarios públicos, manual de funciones, contratos de prestación de servicios	Incumplimiento de las responsabilidades de seguridad de la información asignadas a los funcionarios públicos	1. Falta de competencia de las personas para cumplir con las responsabilidades de seguridad de la información asignadas 2. Desconocimiento de las responsabilidades de seguridad de la información 3. Falta de descripción de los roles y responsabilidades asignadas en los documentos de la contratación	Incumplimiento de la política de seguridad de la información y sanción disciplinaria	Posible	Moderado	Alto
12	Pérdida de Integridad	HARDWARE SOFTWARE Y SERVICIOS	Seguridad de Información	Fallas en servicios de suministro (energía, telecomunicaciones, aire acondicionado)	Daño en equipos informáticos (equipos de cómputo, servidores, equipos de comunicaciones, seguridad, dispositivos móviles)	1. Conexión de equipos a corriente no regulada 2. UPS sin revisión o monitoreo 3. Equipos sin protección contra fallas de energía	Afectación a la disponibilidad de los servicios de Fonprecon	Improblable	Mayor	Alto
13	Pérdida de Disponibilidad	INFORMACIÓN	Seguridad de Información	Funcionarios con roles de seguridad de la información, códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), Atacantes, Proveedores Críticos	Pérdida de la continuidad de la seguridad de la información en situaciones de contingencia	1. Exclusión de la seguridad de la información en la planificación de la continuidad del negocio	Perdida de la continuidad del negocio, servicios afectados para los usuarios internos y externos. Afectación a toda la Entidad	Probable	Catastrófico	Extremo
14	Pérdida de Disponibilidad	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Seguridad de Información	Funcionarios y/o Contratistas, Códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), Atacantes, Proveedores Críticos, infraestructura tecnológica, servicios críticos	Pérdida de la disponibilidad de las instalaciones de procesamiento de información	1. Ausencia de redundancias para los servicios críticos	Perdida de la continuidad de la operación del negocio	Improblable	Mayor	Alto