	GESTIÓN INTEGRAL ORGANIZACIONAL	CODIGO: GIO-PD-02-FT-04
FND Federación Nacional de Departamentos		Versión: 4
	FORMATO MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL	FECHA: 31/03/2023

N°	CAUSAS DESCRIPCIÓN DE LA CAUSA (Debido a.....)	RIESGO	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DESCRIPCIÓN DE LA CONSECUENCIA (Lo que genera.....)	CLASE DE RIESGO	RIESGO INHERENTE				CONTROLES EXISTENTES							RIESGO RESIDUAL				PLAN DE MANEJO DEL RIESGO					SEGUIMIENTO DEL PROCESO			MONITOREO Y REVISION OFICINA CONTROL INTERNO	
						PROBABILIDAD	IMPACTO	NIVEL	VALORACION	DESCRIPCION	TIPO DE CONTROL	DO	AP	EF	EV	PUNTAJE (DO+AP+EF+EV)	PROBABILIDAD	IMPACTO	NIVEL	VALORACION	CONTROL PROPUESTO O ACCIONES A TOMAR	TIPO DE CONTROL	RESPONSABLE		CRONOGRAMA IMPLEMENTACION ACCIONES		INDICADOR PARA LA EVALUACIÓN DE ACCIONES IMPLEMENTADAS	PRIMER CUATRIMESTRE (enero - abril)		FECHA	ACCIONES REALIZADAS
																							CARGO	DEPENDENCIA	INICIA	TERMINA		SEGUIMIENTO	EVIDENCIAS Y/O SOPORTES		
1	1.Debilidad en la aplicación del procedimiento de Control de Acceso. 2. Desconocimiento de las responsabilidades de los colaboradores frente a roles asignados a sus usuarios en los diferentes Sistemas de Información.	1. Acceso a información no autorizada.	Todos los colaboradores de la FND, se les asigana a solicitud del líder del proceso un usuario con roles y permisos de acuerdo a las responsabilidades que cumplen dentro del area. Sin embargo, por desconocimiento se pude presentar prestamos de usuarios entre colaboradores.	1.Manipulacion de información no autorizado. 2. Perdida de información 3. Perdida de credibilidad de la Entidad. 4. Posibles materialización de riesgos.	OPERATIVOS	2	3	6	Moderada	1. Elaboración del Procedimiento de Control de Acceso. 2. Implementación del Procedimiento de Control de Acceso	Preventivo	25	25	25	25	100	1	2	2	Baja	1. Concientizar a los colaboradores FND de la responsabilidad que tienen en el manejo de usuarios asignados en los diferentes Sistemas de Información. 2. Dar a conocer a los colaboradores que los Sistemas de Información de la FND, cuentan con modulo de auditorias donde se puede evidenciar la trazabilidad de las actividades o registros realizados por cada usuario. 3. Solicitud de creacion de usuarios con roles y permisos a través de mesa de ayuda.	Preventivo	Coordinación de Tecnologia	Jefatura Administrativa	1/1/2023	1/12/2023		1. se realizó envio de piezas de sensibilización a los colaboradores en temas de seguridad alineados a la Norma ISO 27001. Ademas de circular por parte de la alta dirección en lineamientos y seguridad de la información. 2. Reporte de Tickets generados en Mesa de ayuda sobre creación de usuarios con roles y permisos en los Diferentes Sistemas de Información.		mayo 15/2023	1. No se puede revisar, realizar seguimiento a los controles debido a que no hay evidencias 2. La matriz no esta diligenciada en su totalidad 3. Revisar los controles, la probabilidad y el impacto y la valoración del riesgo
2	1. Falta de elaboración del Procedimiento Requisitos de Seguridad . 2. Falta de aplicabilidad del Procedimiento Requisitos de Seguridad . 2. Falta de Verificacion de Requisitos de Seguridad en los servicios con los diferentes proveedores.	1. Posible incidencia de Hacking en la entidad.	La Entidad no tine definido la forma de controlar los requisitos de seguridad que deben tenerse en cuenta en los sistemas de información que se adquieren en la organización.	1. Manipulación de información no autorizado. 2. Perdida de información. 3. Perdida de credibilidad de la Entidad.	DE TECNOLOGÍA	3	4	12	Extrema	1. Reglas de Seguridad en Firewall. 2. Diapositivas de Seguridad en el Rack de comunicaciones.	Preventivo	25	25	25	25	100	1	2	4	Baja	1. Implementacion del Protocolo IPV6 en la Entidad. 2. Aprobación de la Politica de Seguridad y Privacidad de la Información . 3. Socialización de la Politica de Seguridad y Privacidad de la Información 4. Segmentación de redes para controlar el acceso a invitados y colaboradores de FND	Preventivo	Coordinación de Tecnologia	Jefatura Administrativa	1/1/2023	1/12/2023		1. La entidad cuenta con protocolo IPV6 implementado. 2. Politica de Seguridad de la Información aprobada y publicada en el SIG 3. Se enviaron piezas de socialización y sensibilidad de la Politica de Seguridad de la Infromación.		mayo 15/2023	1. No se puedenrevisar, realizar seguimiento a los controles debido a que no hay evidencias 2. La matriz no esta diligenciada en su totalidad 3. Revisar los controles, la probabilidad y el impacto y la valoración del riesgo
3	1. Debilidad en la realizacion del respaldo de información de la FND	1. Perdida de información. 2. Reprocesos al interior de la entidad.	Riesgo de perdida de información si no se establecen los controles de seguimiento y verificación de que la información que se maneja en el Drive dispuesta para el almacenamiento de la información no se le hace el respaldo adecuado	1. Perdida de la información. 2. Posible materialización de hallazgos porentes de Control. 3. Afectación reputacional de la entidad.	OPERATIVOS	2	2	4	Baja	1. Realización de respaldo de información almacenada en el Drive de la entidad.	Preventivo	25	25	25	25		1	2	2	Baja	1. El Profesional de Soporte debe notificar a la Coordinadora de Tecnologia que fue realizado el respaldo del Drive y adjuntar evidencia.	Preventivo	Coordinación de Tecnologia	Jefatura Administrativa	1/1/2023	1/12/2023				mayo 15/2023	1. No se puedenrevisar, realizar seguimiento a los controles debido a que no hay evidencias 2. La matriz no esta diligenciada en su totalidad 3. Revisar los controles, la probabilidad y el impacto y la valoración del riesgo
4	1. Indisponibilidad en los Sistemas de Información contratados con terceros	1. Perdida de disponibilidad de la información.	Los Sistemas de Información de la FND son sumistrados a través de contratación con terceros, si no se realiza estricta verificacion en los acuerdos de disponibilidad de servicios se corre riesgos de disponibilidad de información	1. Indisponibilidad de la información. 2. Posible materialización de hallazgos porentes de Control. 3. Afectación reputacional de la entidad.	DE TECNOLOGÍA	2	3	6	Moderada	1. Los ANS hacen parte integral de los contratos de la Coordinación de Tecnologia. 2. Seguimiento al cumplimiento de envio de copias de seguridad de informacion con los diferentes proveedores	Preventivo	25	25	25	25	100	1	2	2	Baja	1. Se implemento el Procedimiento de Plan de Continuidad. 2. Actualización e implementación del Formato Registro de Copias de Seguridad	Preventivo	Coordinación de Tecnologia	Jefatura Administrativa	1/1/2023	1/12/2023		1. Se actualizó el Procedimiento de Plan de Continuidad. 2. Se llevan los registros de las copias de seguridad enviados por los proveedores de los Sistemas de Información (Sysman - Az Digital)		mayo 15/2023	1. No se puedenrevisar, realizar seguimiento a los controles debido a que no hay evidencias 2. La matriz no esta diligenciada en su totalidad 3. Revisar los controles, la probabilidad y el impacto y la valoración del riesgo

Nota: Todos los riesgos asociados con salud y seguridad en el trabajo (identificación de peligros y evaluación de los riesgos), para cada proceso se encuentran establecidos en la FORMATO MATRIZ IDENTIFICACIÓN DE PELIGROS, EVALUACIÓN Y CONTROL DE LOS RIESGOS , donde se evidencia la implementación de los controles aplicables y son gestionados por el área SST de GRH.