

MAPA DE RIESGOS 2020

CAJA DE SUELDOS DE RETIRO DE LA POLICIA NACIONAL
 MAPA DE RIESGOS SEGURIDAD DE LA INFORMACION
 VIGENCIA : 2020



N° RIESGO	PROCESO Y OBJETIVO / SISTEMA	RIESGO DEFINIDO	TIPO DE RIESGO	SOLO APLICAN PARA RIESGO DE SEGURIDAD DE LA INFORMACION		CAUSAS/ VULNERABILIDADES	CONSECUENCIAS	CONTROLES	SOLO APLICA PARA RIESGOS DE SEGURIDAD DE LA INFORMACION CONTROLES ANEXO A 27001	NATURALEZA DEL CONTROL (PREVENTIVO-DETECTIVO-PREDICTIVO)	PLAN DE TRATAMIENTO O MITIGACION				
				ACTIVO	TIPO DE ACTIVO						ACCIONES DE CONTROL	REGISTRO O SOPORTE	FECHA DE INICIO	FECHA DE FINALIZACIÓN	RESPONSABLE DE LA ACCION
1		Incumplimiento de los procedimientos en los Sistemas de información. (SINPRES, ERP DI EDWARDS, HYPERION CONTROLDOC e IVR)	disponibilidad	Base de datos de CONTROLDOC	Software	Debilidad en el conocimiento en tecnologías de la información	Hallazgos y/o observaciones por entes de control internos y externos	Manual de políticas de administración de seguridad de la información	A.5.1_Directrices_establecidas_por_la_dirección_para_la_seguridad_de_la_información	Preventivo	Creacion del repositorio de los manuales y/o instructivo de los sistemas de información	ACTA	03-feb-20	31-dic-20	Grupo de Informatica
				Base de datos misional Oracle 10G	Software		Incumplimiento de la estrategia, los objetivos, planes y programas	Acta de Aceptación Políticas de Seguridad de la información	A.5.1.1_Políticas_para_la_seguridad_de_la_información	Preventivo					
				CONTROLDOC	Software	déficit de personal capacitado para atender los requerimientos de la entidad ante la ausencia de los titulares de los procesos	Insatisfacción de los Grupos Sociales Objetivo	Procedimiento Gestión del conocimiento y procedimiento gestión de cambio.	A.12.1.1_Procedimientos_de_operación_documentados	Preventivo	Difundir la creacion del repositorio documental de los software de la entidad.	ACTA	03-feb-20	31-dic-20	Grupo de Informatica
				Portal Web	Software	Impericia en el manejo de los Sistemas de Información.	Investigaciones Administrativas, Disciplinarias, Fiscales, Penales.	Procedimiento de inducción y reintroducción	A.9.2_Gestión_de_acceso_de_usuarios	Preventivo					
				Servidor virtual	Software	Falta de conocimiento de las actividades del proceso	Pérdida de credibilidad e imagen del proceso y/o la Entidad	Procedimiento de inducción y reintroducción	A.12.1.1_Procedimientos_de_operación_documentados	Preventivo	Realizan una campaña de apropiación de las políticas de seguridad en la información	ACTA	03-feb-20	31-dic-20	Grupo de Informatica
		Ausencia de personal de respaldo para los roles y responsabilidades.	Pérdidas económicas y/o sobre costos por inoperatividad de los procesos	Procedimiento gestion del conocimiento, procedimiento gestion de cambio	A.6.1.1_Roles_y_responsabilidades_para_la_seguridad_de_información	Preventivo									
2		Ataque Informatico	disponibilidad	SINPRES	Software	Debilidades en la apropiación de políticas de seguridad de la información	Hallazgos y/o observaciones por entes de control internos y externos	Acta de Aceptación Políticas de Seguridad de la información.	A.5.1.1_Políticas_para_la_seguridad_de_la_información	Preventivo	Realizar el seguimiento a los reportes mensuales del anti-virus de la entidad	Informe	03-feb-20	31-dic-20	Grupo de Informatica
							Acción indebida de los funcionarios con privilegios de acceso	Incumplimiento de la estrategia, los objetivos, planes y programas	Procedimiento de gestión de usuarios, formato de usuarios y formato de excepciones.	A.9.4,1 Restricción de acceso a la información.					
				GD EDWARDS	Software	Accesos no autorizados locales y remotos	Investigaciones Administrativas, Disciplinarias, Fiscales, Penales	Procedimiento de gestión de usuarios, formato de usuarios y formato de excepciones.	A.6.1.5_Seguridad_de_la_información_en_la_gestión_de_proyectos	Preventivo	Fortalecer trimestralmente los controles de seguridad perimetral	Informe	03-feb-20	31-dic-20	Grupo de Informatica
						Cifrado no autorizado provocado por malware	Pérdida de credibilidad e imagen del proceso y/o la Entidad	Controles seguridad perimetral	A.16,1,1 Responsabilidades y Procedimientos	Detectivo					

3	Interrupción de la Operación de la Plataforma Tecnológica	disponibilidad	Hyperion	Software	Acceso sin autorización locales, remotos y a los centros de cableado o de la UPS,	Hallazgos y/o observaciones por entes de control internos y externos	Manual de políticas y administración de seguridad de la información	A.12.1.1_Procedimientos_d e_operación_documentados	Preventivo	Ampliar la cobertura del sistema de continuidad de negocio (DRP) en dos sistemas de información	informe	03-feb-20	31-dic-20	Grupo de Informatica
			IVR	Software	Falta de mantenimiento de la plataforma tecnológica	Incumplimiento de la estrategia, los objetivos planes y programas	Plan de Mantenimiento infraestructura tecnológica plan de compras - Plan de Necesidades	A.14_Adquisición_desarroll o_y_mantenimientos_de_sistemas	Preventivo					
			Almacenamiento SAN	Hardware	Ocurrencia de hechos fortuitos o malintencionados en los centros de computo.	Insatisfacción de los Grupos Sociales Objetivo	Procedimiento de compras Plan de contingencia	A.13,1,2 Seguridad de los Servicios de Red.	Preventivo					
			Planta Telefonica	Hardware	Debilidad en la infraestructura tecnológica	Investigaciones Administrativas, Disciplinarias, Fiscales, Penales	Plan de mantenimiento de la infraestructura - Plan de compras - Plan de Necesidades	A.14,1,3 Protección de Transacciones de los servicios de las aplicaciones.	Preventivo					
			Servidores Fisicos	Hardware	Intrusión de personal no autorizado a la plataforma tecnológica	Pérdida de credibilidad e imagen del proceso y/o la Entidad	Procedimiento gestion de usuarios	A.9,2_Gestión_de_acceso_d e_usuarios	Preventivo					
			UTM Fortigate	Hardware	Interrupción de los servicios prestados por terceros. (redes eléctricas, comunicaciones de voz y datos)	Pérdidas económicas y/o sobre costos por inoperatividad de los procesos	Procedimiento de gestión de usuarios, formato de gestión de usuarios y formato de excepciones.	A.13,1,2 Seguridad de los Servicios de Red	Preventivo					
			Token	Hardware	Aplicación inadecuada de los controles del proceso y procedimientos.	Sanciones Disciplinarias Penales Fiscales	Procedimiento de inducción y reinducción	A.12.1.1_Procedimientos_d e_operación_documentados	Preventivo					
4	Pérdida, alteración o sustracción de Información en medio magnético o físico.	Confidencialidad	Historias Laborales	Información Física Digital	Falta control de acceso a la información	Hallazgos y/o observaciones por entes de control internos y externos	Procedimiento de gestión de usuarios, formato de gestión de usuarios y formato de excepciones.	A.7.2_Durante_la_ejecución _del_empleo	Preventivo	Actualizar el Programa de gestion documental de	informe	03-feb-20	30-abr-20	Coordinador grupo de informacion documental
					Falta de valores y compromiso con la Entidad	Incumplimiento de la estrategia, los objetivos planes y programas	Código de ética de Integridad y Buen Gobierno	A.7.2.2_Toma_de_conciencia_educación_y_formación_en_la_seguridad_de_la_información	Preventivo					
					Manipulación indebida de los documentos de archivo y uso inadecuado de los aplicativos.	Insatisfacción de los Grupos Sociales Objetivo	Programa de gestión documental	A 11,1,3 Seguridad de oficinas, recintos e instalaciones.	Preventivo					
			Expedientes Disciplinarios	Información Física Digital	Perfil inadecuado de los servidores públicos que intervienen en el procedimiento	Investigaciones Administrativas, Disciplinarias, Fiscales, Penales	Procedimiento de Selección	A 7,1,1 Selección	Preventivo	Realizar la inducción y reinducción de contratistas y/o servidores públicos al inicio de la vinculación laboral como durante la misma	Acta y Formato de Inducción	02-feb-20	28-feb-20	Coordinador de GCID
					Intereses a favor de terceros	Pérdida de credibilidad e imagen del proceso y/o la Entidad	Formatos de consulta prestamos de información o documentación.	A.8.1.3_Us o_aceptable_de_los_activos	Preventivo	Divulgar a los colaboradores el formato estandar de acuerdo de confidencialidad al iniciar la prestación de sus servicios	Acuerdo firmado	02-feb-20	28-feb-20	Coordinador de GCID
					Indebida manipulación de la documentación recepcionada por el personal de la Entidad.	Pérdidas económicas y/o sobre costos por inoperatividad de los procesos	Procedimiento Control de Acceso	A.12.1.1_Procedimientos_d e_operación_documentados	Preventivo	Participación de cursos virtuales o presenciales gratuitos de integridad y ética, y posterior socialización al interior del grupo.	Certificado o constancia	02-mar-20	30-nov-20	Coordinador de GCID

SISTEMA SEGURIDAD DE LA INFORMACION
GESTION DE LAS TIC
GESTION CONTRACTUAL
GESTION FINANCIERA
GESTION DEL TALENTO HUMANO
GESTION JURIDICA

5	Alteración, divulgación o uso mal intencionado de información sensible para la Entidad.	Confidencialidad	Certificaciones de disponibilidad presupuestal	Información Física Digital	Incumplimiento de compromiso de confidencialidad	Sanciones Disciplinarias Penales Fiscales	Acuerdos de confidencialidad	A, 13,2,4 Acuerdos de confidencialidad o de no divulgación.	Preventivo	Comparar aleatoriamente de manera trimestralmente a los CDP Y CRP generados por el SIF Nacion (reporte) con los impresos archivos en la entidad debidamente firmados	Acta	03-feb-20	31-dic-20	Grupo de Presupuesto		
			Registros Presupuestales.		Incumplimiento de los Roles y Responsabilidades para la seguridad de la Información.		acta de aceptación de Políticas de Seguridad de la Información.		Preventivo							
			Manejo indebido en la organización de la documentación producida por el Grupo		Formato devolución y entrega de documentos a través del aplicativo de Gestión Documental y/o por libro		A 6,1,1 Roles y Responsabilidades para la seguridad de la información.		Preventivo		Socializar al interior del grupo de presupuesto las capacitaciones asistidas por los servidores publicos en el Minhacienta - sobre los temas SIF Nación.	ACTA TRIMESTRAL	03-feb-20	15-dic-20	Grupo de Presupuesto	
				Prestatamo y/o uso inadecuado de los claves asignadas								Inducción y reinducción al interior del proceso del procedimiento Gastos SIF Nación Transversal	ACTAS TRIMESTRAL	17-feb-20	15-dic-20	Grupo de Presupuesto
			Análisis Jurídicos	Información Física Digital	Actos desleales por parte de los colaboradores del proceso afectando la integridad del documento.	Hallazgos y/o observaciones por entes de control internos y externos	Acta de Aceptación Políticas de Seguridad de la información. Manual de políticas y administración de seguridad de la información	A.16,1,1 Responsabilidades y Procedimientos .	Preventivo	Alimentacion de manera trimestral del back up de conceptos jurídicos, emitidos por parte de la Oficina Asesor jurídica	Registro del up-Conceptos jurídicos.	01-feb-20	31-dic-20	JEFE OFICINA ASESORIA JURIDICA.		
			Creditos Hipotecarios	Información Física Digital	Incumplimiento de los procedimientos del proceso de apoyo de gestión jurídica	Incumplimiento de la estrategia, los objetivos, planes y programas	Socialización a los colaboradores del proceso respecto de la totalidad de los procedimientos con los que cuenta la gestión jurídica	A.12.1.1_Procedimientos_d e_operación_documentados	Detectivo	Sensibilización de los procedimientos documentales de manera trimestral a la totalidad de los colaboradores respecto del debido manejo de la información, los lineamientos establecidos por la Entidad y las consecuencias (penales, disciplinarias y fiscales) que se puedan derivar de la Alteración, divulgación o uso mal intencionado de información sensible para la Entidad	Sensibilizaciones Realizadas	01-feb-20	31-dic-20	JEFE OFICINA ASESORIA JURIDICA.		
			Base de datos del directorio activo.	Información Física Digital	Aplicación inadecuada de los controles del proceso y procedimientos.	Insatisfacción de los Grupos Sociales Objetivo	Procedimientos documentados, Manual de Políticas de Seguridad	A.9,3,1 Uso de información de autenticación secreta.	Preventivo							
			Bases de Datos administrativas y financieras.	Información Física Digital	Interrupción de los servicios prestados por terceros. (redes eléctricas, comunicaciones de voz y datos). Ataque informático interno por parte de un funcionario o contratista con acceso, a la plataforma tecnológica	Investigaciones Administrativas, Disciplinarias, Fiscales, Penales	Procedimiento Radicación y trámite de comunicaciones oficiales para cada proceso.	A 7,2,2 Toma de conciencia, educación y formación en la seguridad de la información	Preventivo	Actualizar el Programa de gestion documental	informe	03-feb-20	30-abr-20	Coordinador grupo de informacion documental		
			Expedientes prestacionales	Información Física Digital	Incumplimiento de los procedimientos documentales	Pérdida de credibilidad e imagen del proceso y/o la Entidad	Plan de capacitación	A 7,2,2 Toma de conciencia, educación y formación en la seguridad de la información	Preventivo	Ejecutar el plan de institucional de archivo propuesto para la vigencia 2020	informe cumplimiento	03-feb-20	31-dic-20	Coordinador grupo de informacion documental		
					Revelar información confidencial para producir resultados, con tendencias específicas.	Pérdidas económicas y/o sobre costos por inoperatividad de los procesos	Procedimiento de inducción y reinducción		Preventivo	Incluir en el sistema JD los archivos planos correspondientes de cada pago bancario para que éstos se generen directamente para ser transmitidos a las entidades bancarias.	Acta	01-ene-20	30-jun-20	Coordinador Grupo Tesorería		
Registro bancario	Información Física Digital						Socializar los lineamientos del manual de políticas del manejo de los token verificando con los perfiles y transacción de cada usuario del grupo.	Acta	01-ene-20	31-mar-20	Coordinador Grupo Tesorería					
	Información Física Digital	Conductas no apropiadas por carga de trabajo y componente emocional	Sanciones Disciplinarias Penales Fiscales	Plan de capacitación	A.12.1.1_Procedimientos_d e_operación_documentados	Preventivo	Capacitar a los servidores del grupo de tesorería con respecto a los módulos establecidos por los procedimientos del siif nación.	Acta	01-ene-20	30-ago-20	Coordinador Grupo Tesorería					
							Sensibilizar las Políticas de seguridad de la información	Acta	01-feb-20	30-sep-20	Coordinador Grupo Tesorería					
							Socializar los formatos gestión de usuarios, formato de excepciones con los servidores del grupo.	Acta	02-ene-20	30-oct-20	Coordinador Grupo Tesorería					

6	Grabación Erronea de datos en el sistema prestacional	integridad	Novedades de Nomina	Información Física Digital	Fallas en el origen de la novedad (donde se creo el documento)	Pérdidas económicas y/o sobre costos por inoperatividad de los procesos	Reparto de expediente, de acuerdo con la experiencia del servidor publico	A.7,2,2 Toma de Conciencia, educación y formación en la seguridad de la Información	Preventivo	Reinducción en analisis y valoracion del registro de las novedades, actualización normas	Acta	01-jul-20	31-oct-20	Coordinador Grupo Nominas y Embargos
					Desconocimiento a la inter-operatividad del sistema	Sanciones Disciplinarias Penales Fiscales	Revisión de pre-nómina	A.18,2,1 Revisión Independiente de la Seguridad de la Información.	Detectivo					
					Falla en el Analisis de las novedades de nomina.	Pérdida de credibilidad e imagen del proceso y/o la Entidad	Chequeo cruzado de grabación	A.18,2,2 Cumplimiento con las Políticas y normas de Seguridad.	Detectivo	Mesa de trabajo con junta con prestaciones sociales y oficina Jurídica, para analisis, corrección y disminucion de devoluciones de novedades de nomina	Acta	01-ago-20	31-dic-20	Coordinador Grupo Nominas y Embargos
							Devolución de Inconsistencias	A.12.1.1_Procedimientos_d e_operación_documentados	Detectivo					
procedimiento gestión de usuarios				Detectivo	Implementacion de interoperabilidad con policia nacional para registro automatico de datosde datos	Acta	01-feb-20	30-jun-20	Coordinador Grupo Nominas y Embargos					