PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2021

Aprobado CIGD Nro. 1 - 2021-01-29

Convenciones
Riesgos emergentes
Gestión riesgos plan 2020

Item	Riesgos / Actividad	Riesgo asociado en matriz de riesgos institucionales	Acciones / Tareas	Entregable	Responsables	Estado	Mes											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	Actualización del mapa de riesgos en Seguridad de la Información. Insumos: 1. Matriz de riesgo actual 2. Incidentes (riesgos materializados) 2. Consultoría EDURED	N.A.	Actualización de la matriz, partiendo de los riesgos identificados en 2019 y gestionados en 2020. (requisito).	Imagen de los riesgos actualizados en Isolución.	Oscar Ramírez / Omar E Mejía	Planeado		X	X									
2	Hackeo Página Web (Riesgo materializado).	N.A.	1. Realización de analisis de riesgo (identificacion causas). 2. Revisión medidas de seguridad contractuales. 3. Evaluación seguridad del hosting (plataforma) y aplicación post incidente.	Informe de Riesgos y Recomendaciones plan de acción.	Oscar Ramírez / Omar E Mejía	En ejecución	X											
3	Seguimiento a riesgos de seguridad de la información por trabajo en casa.	N.A.	1. Actualización del analisis de riesgos. (incidentes, impacto). 2. Evaluación controles implementados	Informe de Riesgos y recomendaciones plan de acción.	Oscar Ramírez / Omar E Mejía	Planeado		X										
1	Herramientas de protección informática frente a amenazas identificadas (no disponer de éstas).	E05-R04	1. Identificar y adquirir herramientas informáticas para la protección ante posibles amenazas existentes. 2. Definir e implementar políticas para la seguridad de la información.	1. Herramientas implementadas. (plataforma Fortinet) 2. Manual del SGSI con políticas.	1. Omar E Mejía 2. Oscar Ramírez	1. Implementado 2. Implementado												
2	Información en Aplicativos y Desarrollos (afectación por daños físicos sobre la infraestructura tecnológica, ataques informáticos, por inyección de código, con las debilidades en la programación).	E05-R05	1. Configurar los ambientes de desarrollo y pruebas en servidor de aplicaciones principal y alterno ▪ Restricción de acceso Información ▪ Actualizar y mantener el sistema de respaldo (Backus) de los aplicativos de la entidad. 2. Ubicar y proteger los equipos ▪ Elementos de protección/control ambiental, registros de mantenimiento ▪ Perímetro de seguridad física Propósito: Definición del perímetro de seguridad, de acuerdo a su ubicación, accesos físicos restringidos	1. Separación de ambientes de desarrollo y pruebas. 2. Restricción de acceso. 3. Actualizar y mantener sistema de respaldo. (backups). 4. Controles ambientales 5. Mantenimiento a equipos 6. Acceso fisico restringido.	Jefe de Oficina	1. Implementado (ej BPMetro) 2 a 6 Implementado												
3	Software desactualizado para la operación de los procesos del INM. (versiones de software obsoletas o sin soportes).	E05-R01	1. Hacer seguimiento a través de inventarios al software implementado 2. Elaborar propuesta de Migración de Aplicaciones	Se instalaron nuevos programas como BPMetro y se renovó el soporte de software	Jefe de Oficina	Cumplido / Permanente												

4	Exposición ante nuevas amenazas informáticas. (Hace referencia principalmente a la reacción para brindar protección a la información del INM ante nuevos ataques informáticos a raíz de la ausencia y debilidades en los lineamientos frente a la confidencialidad y no divulgación).	E05-R07	Establecer restricciones de acceso a la Información	1. Controles de acceso a la información (En 2020 mejoras al formato de permisos y depuración de accesos). 2. Acuerdos de confidencialidad 3. Procedimiento de control de acceso (POSI 2021)	1. Mesa de servicios 2-3. Omar Mejía / Oscar Ramírez	1. Cumplido 2. Planeada revisión 3. Planeado			**2.X**					**3.X**	**3.X**			
5	Hardware desactualizado para la operación de los procesos del INM	E05-R02	1. Elaborar Inventario de hardware donde se evidencien los ciclos de vida de equipos (Equipos de computo, impresoras, servidores, telefonía, switches etc.) 2. Generar reporte del Estado de Hardware utilizado en el INM	Renovación tecnológica del hardware. (PC) y red inalambrica	Omar Mejía	Cumplido															
6	Almacenamiento y respaldo de la información, ante las necesidades del INM. (perdida de la información, ocasionada por daños físicos, falta o incumplimiento de políticas de respaldo (BackUp), durante mantenimientos, fallas físicas, eventos naturales y manipulación inadecuada de medios magnéticos)	E05-R11	1. Reforzar el conocimiento y aplicación de políticas y buenas practicas de respaldo de la información. 2. Capacitar al personal en Buenas Prácticas de Análisis Forense y Cadena de Custodia	1. Actualización del procedimiento de back ups y políticas al respecto. 2. Evidencias de capacitación	1. Omar Mejía 2. Oscar Ramírez	1. Cumplido. 2. A revisión.															