# GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

| IDENTIFICACIÓN | | | | | | | | CALIFICACIÓN | | | | VALORACIÓN | | | | | | | | PLAN DE TRATAMIENTO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| COMPONENTE DEL SIG | TIPO DE PROCESO | PROCESO | OBJETIVO DEL PROCESO | RIESGO | CAUSAS O EVENTOS | TIPO DE RIESGO | CONSECUENCIAS (RESULTADO DEL EVENTO) | PROBABILIDAD ESCALA<br>RARA VEZ = 1<br>IMPROBABLE = 2<br>POSIBLE = 3<br>PROBABLE = 4<br>CASI SEGURO = 5 | IMPACTO ESCALA<br>INSIGNIFICANTE = 3<br>MENOR = 6<br>MODERADO = 9<br>MAYOR = 12<br>CATASTROFICO = 15 | EVALUACION DEL RIESGO INHERENTE (PROBABILIDAD X IMPACTO) | NIVEL DE RIESGO INHERENTE (RIESGOS PROPIOS DEL PROCESO O ACTIVIDAD) | CONTROLES EXISTENTES (SE DETALLAN LOS CONTROLES EXISTENTE) | CANT. DE CONTROLES EXISTENTES (SE SUMAN LOS # DE CONTROLES EXISTENTES REFIERE COLUMNA N) | TIPO DE CONTROL<br>1= INEXISTENTE<br>2= DETECTIVO<br>3= CORRECTIVO<br>4= PREVENTIVO | PERIODICIDAD DEL CONTROL<br>1= OCASIONAL<br>2= PERIÓDICO<br>3= PERMANENTE | PRODUCTO (TIPO DE CONTROL X PERIODICIDAD DEL CONTROL) | EFICACIA DEL CONTROL | VALORACION DEL CONTROL (EFICACIA DEL CONTROL EN TÉRMINOS CUALITATIVOS) | NIVEL DE RIESGO RESIDUAL ESCALA<br>EXTREMO<br>ALTO<br>MODERADO<br>BAJO | OPCIÓN DE TRATAMIENTO (MITIGAR /ASUMIR /EVITAR / /TRASNFERIR) | ACCIONES (CONTROL EFECTIVO FUTURO A IMPLEMENTAR) (DETALLAR PLAN DE ACCIÓN EN TÉRMINOS DEL CICLO PVHA) | RESPONSABLE (DEL TRATAMIENTO DEL RIESGO) | CRONOGRAMA DEL PLAN DE ACCIÓN<br>FECHA INICIO (dd/mm/aaaa) | FECHA FIN (dd/mm/aaaa) |
| | | | | | | | | | | | | | | | | | | | | | | | | |
| Sistema de Gestión de Seguridad de Información (SGSI) | Proceso_Estratégico | Planeación Institucional | Planeación | Posibilidad de comprometer la **integridad** de la información institucional debido a fallas técnicas y operativas en el proceso. | * (Tecnologia) Ausencia de manuales de uso<br>* (Tecnologia) Ciberataques<br>* (Tecnologia) Plataforma tecnológica obsoleta<br>*(Procesos) Acceso no autorizado la información.<br>*(Personal) Errores humanos | Seguridad Digital | * Inconsistencias en la calidad de la información y reprocesos.<br>* Afectación en la comunicación de los servicios.<br>* Inadecuada toma de decisiones.<br>* Perdida reputacional.<br>* Incumplimiento normativo<br>* Procesos administrativos y/o judiciales | 3 | 12 | 36 | ALTO | Acceso a la informacion con usuarios y claves.<br>Roles y privilegios<br>Identificacion de los activos de informacion<br>Politicas de control de acceso<br>Politicas de seguridad de la informacion | 5 | 4 | 3 | 12 | 4 | ALTO | MODERADO | Mitigar el Riesgo | P: Solicitar charla de socialización de las politicas de seguridad de la informacion para que todo el personal del proceso las conozcan y las cumplan.<br><br>Participar en las sesiones de induccion y reinducion<br><br>Solicitar charlas relacionadas con uso y apropiacion de las herramientas tecnologicas. | El proceso<br><br>Comunicaciones. | P:<br>H:<br>V:<br>A: | P:<br>H:<br>V:<br>A: |
| Sistema de Gestión de Seguridad de Información (SGSI) | | | | Posibilidad de comprometer la **confidencialidad** de la información institucional debido a fallas técnicas y operativas en el proceso. | *(Personal) Trabajo de personal externo o de mantenimiento no supervisado.<br>*(Procesos) Carencia de procedimientos adecuados de reutilización de medios, computadores y disposición final de medio de almacenamiento (Fisico y digital).<br>*(Procesos) Desconocimiento o falta de capacitación en seguridad de la información<br>*(Procesos) Equipos de cómputo desatendidos<br>*(Procesos) Errores en la definición de roles en las aplicaciones.<br>*(Tecnología) Falta de aplicación de buenas prácticas en la configuración de aplicaciones.<br>*(Procesos) Falta de capacitación de los usuarios de acuerdo con su rol.<br>*(Procesos) Falta de capacitación para las funciones asignadas.<br>*(Procesos) Falta de seguimiento a los controles de acceso a la información<br>*(Procesos) Falta de divulgación de las políticas, normas y procedimientos de seguridad de la información.<br>*(Tecnología) Solución de antivirus y código malicioso desactualizada (ataque por nuevas amenazas)<br>*(Procesos) Falta de revocación de los derechos de acceso al activo de información una vez el funcionario cambie de rol o se retire de la organización.<br>Controles de acceso debiles | Seguridad Digital | | | | | #N/D | 1. Polìitcas de Seguridad.<br>2. Politicas TI.<br>3. Documentacion (Procedimientos-formatos-instructivos).<br>4. Segmentación de RED.<br>5. Areas Seguras definidas.<br>6. Usuarios con acceso logico. | | | | 0 | #N/D | | | | | | P:<br>H:<br>V:<br>A: | P:<br>H:<br>V:<br>A: |
| Sistema de Gestión de Seguridad de Información (SGSI) | | | | Posibilidad de comprometer la **disponibilidad** por dependencia (parcial o total) tecnológica de los proveedores de servicios TICS | *(Tecnología) Dependencia tecnológica de los proveedores de las herramientas.<br>*(Tecnología) Limitada capacidad de respuesta frente a eventualidades, urgencias, incidencias y requerimientos por parte de TICS<br>*(Procesos) Debilidad en la socialización de las actualizaciones a los sistemas<br>*(Financieros) Limitada asignación de recursos presupuestales para la ejecución de los planes asociados al proceso | Seguridad Digital | | | | | #N/D | | | | | 0 | #N/D | | | | | | P:<br>H:<br>V:<br>A: | P:<br>H:<br>V:<br>A: |
| Sistema de Gestión de Seguridad de Información (SGSI) | | | | Posibilidad de no atender las necesidades de automatización de los procesos de la entidad, debido a capacidad limitada de los productos adquiridos | *(Tecnología) Los proveedores son los dueños del código fuente de los aplicativos, y del conocimiento de los mismos; si para continuidad del negocio necesariamente se les debe contratar porque son los únicos que pueden dar soporte y mantenimiento por fallos del mismo, y/o actualizaciones requeridas al producto<br>*(Tecnología) Algunos servicios Tic que soportan la operación de la entidad son especializados y no se cuenta con las capacidades para atenderlos adecuadamente, por lo que se tercerizan<br>*(Tecnología) Contratación de productos TICS con especificaciones generales frente a las necesidades puntuales de la entidad, evidenciado en el momento de entrega de los mismos | Seguridad Digital | | | | | #N/D | | | | | 0 | #N/D | | | | | | P:<br>H:<br>V:<br>A: | P:<br>H:<br>V:<br>A: |
| Sistema de Gestión de Seguridad de Información (SGSI) | | | | Posibilidad de tener Sistemas de información desatendidos o sin soporte debido a la imposibilidad de continuidad a los contratos de soporte y mantenimiento | *(Tecnología) El fabricante del sistema de información está sancionado para contratar con entidades del Estado<br>*(Financieros) Falta de recurso para dar continuidad a contratos de soporte y mantenimiento | Seguridad Digital | | | | | #N/D | | | | | 0 | #N/D | | | | | | P:<br>H:<br>V:<br>A: | P:<br>H:<br>V:<br>A: |
| Sistema de Gestión de Seguridad de Información (SGSI) | | | | Posibilidad de tener afectacion de integridad, confidencilaid y/o disponibilidad de la informacion por errores humanos | Desconocimiento de los lineamientos del SGSI (politicas, normas y procedimientos).<br>Ausencia de personal que cumpla con los Roles establecidos en la guía de roles de Servicios Tecnológicos de la Estrategia de gobierno en Linea.<br>Falta de uso y apropiacion en cultura organizacional en seguridad de la informacion.<br>Incumplimiento y/o desactualización de los Procesos y procedimientos relacionados con Gestión de TICS.<br>Inadecuado manejo de la información causada por una indebida manipulación de los custodios<br>Abuso de derechos<br>Copia no autorizada de información<br>Modiifcación no aupotrizada de informacion.<br>Ausencia de personal.<br>Uso no autorizado de equipos<br>Servidor publico insatisfecho<br>Exceso de confianza | Seguridad Digital | | | | | #N/D | | | | | 0 | #N/D | | | | | | P:<br>H:<br>V:<br>A: | P:<br>H:<br>V:<br>A: |