|  |  |
| --- | --- |
| **LISTA DE REQUERIMIENTOS FUNCIONALES** | |
| **Código** | **Descripción** |
| RF01 | El sistema debe permitir la creación, modificación, y eliminación de usuarios, incluyendo la asignación de roles y permisos. |
| RF02 | El sistema debe permitir la creación y gestión de roles y permisos, asegurando que los usuarios solo accedan a las funciones necesarias para su rol. |
| RF03 | El sistema debe facilitar la creación y documentación del inventario de procesos, incluyendo la asignación de responsables y recursos, con capacidades de navegación clara entre los procesos definidos. |
| RF04 | El sistema debe permitir el registro, actualización y consulta de matrices de caracterización de procesos, incluyendo entradas, salidas, indicadores y recursos. |
| RF05 | El sistema debe permitir el seguimiento y análisis del desempeño de los procesos definidos, mostrando indicadores clave y facilitando la toma de decisiones. |
| RF06 | El sistema debe permitir el registro y aprobación de solicitudes de modificación de procesos, asegurando que los cambios sean documentados y aprobados adecuadamente antes de su implementación. |
| RF07 | El sistema debe permitir la programación y planificación de auditorías internas y externas, incluyendo la asignación de auditores, definición del alcance, procesos a ser auditados, criterio de auditorías, horario, y cualquier detalle necesario para su ejecución.  El sistema debe permitir contar con un directorio de auditores el cual permita su ingreso, modificación o baja de auditor, y deberá permitir ser insumo para la planificación de las auditorías. |
| RF08 | El sistema debe facilitar la realización de auditorías, registro de hallazgos, generación de informes de auditoría y su notificación. |
| RF09 | El sistema debe permitir el registro y categorización de hallazgos de auditoría, con su respectivo analisis de causas |
| RF10 | El sistema debe facilitar la creación, asignación, seguimiento y cierre de acciones correctivas derivadas de los hallazgos, permitiendo adjuntar archivos que servirán como evidencias del desarrollo de las acciones.  El sistema debe permitir programar las fechas para la evaluación de eficacias las acciones correctivas, en caso de que la evaluación sea negativa, el sistema solicitará el establecimiento un nuevo hallazgo. |
| RF11 | El sistema debe permitir registrar, editar y/o eliminar perspectivas relacionadas con el análisis del contexto interno y externo. |
| RF12 | El sistema debe permitir la identificación, evaluación, y monitoreo de riesgos, con la asignación y registro de controles.  El sistema debe permitir programar las fechas para la evaluación de eficacias de los controles, en caso de que la evaluación sea negativa, el sistema solicitará el establecimiento nuevas acciones. |
| RF13 | El sistema debe permitir programar las fechas para la revisión y monitoreo de controles, así como los comentarios o resultados producto de esta evaluación.  En caso de que la evaluación sea negativa, el sistema solicitará el establecimiento de un nuevo control. |
| RF14 | El sistema debe facilitar la creación, asignación, seguimiento y cierre de acciones derivadas de los planes de tratamiento de riesgos, permitiendo adjuntar archivos que servirán como evidencias del desarrollo de estas acciones. |
| RF15 | El sistema debe permitir el registro y seguimiento de incidentes de seguridad de la información. |
| RF16 | El sistema debe permitir la creación, distribución, y análisis de encuestas de satisfacción. |
| RF17 | El sistema debe permitir la creación, edición, aprobación, eliminación y publicación de los documentos del SIG (procedimientos, manuales, guías, instructivos, entre otros), permitiendo adjuntar archivos y controlando las versiones de los documentos. |
| RF18 | El sistema debe permitir el registro de las principales obligaciones de cumplimiento y de sus controles a efectos de evaluar las consecuencias de su incumplimiento. |
| RF 19 | El sistema debe permitir el registro y monitoreo del cumplimiento de requisitos legales y normativos, que permita alertar a los usuarios sobre vencimientos o cambios regulatorios que afecten el SIG. |
| RF 20 | El sistema debe integrarse con plataformas como SharePoint o Google Drive para la gestión de documentos y colaboración. |
| RF 21 | El sistema debe enviar notificaciones automáticas para recordatorios y seguimientos de acciones pendientes para los planes de tratamiento de riesgos y hallazgos. |
| RF 22 | El sistema debe contar con un historial de versiones de la documentación de procesos, contexto interno y externo, programa anual de auditorías, plan de auditorías, y otros documentos que forman parte de la gestión documental. |
| RF 23 | El sistema debe permitir generar reportes personalizados (incluir gráficos y demás dashboards según las necesidades de cada tipo de actor o usuario |
| RF 24 | El sistema debe permitir la gestión de competencias del personal, registrando participaciones den charlas de sensibilización, capacitaciones y su seguimiento, asegurando el cumplimiento de los requisitos de toma de conciencia para cada norma. |
| RF 25 | El sistema debe permitir registrar las decisiones tomadas durante la revisión por la dirección y facilitar el seguimiento de las acciones derivadas de esas decisiones, asignando responsables y plazos. |
| RF 26 | El sistema debe enviar notificaciones automáticas a los responsables de cada área para la preparación y entrega de información necesaria antes de la revisión por la dirección. |
| RF 27 | El sistema debe permitir el registro y categorización de salidas no conformes, ya sea de productos, servicios o procesos. Este registro debe incluir detalles como la naturaleza de la no conformidad, el proceso afectado, responsable, fecha de detección, impacto y acciones inmediatas tomadas. |

|  |  |
| --- | --- |
| **LISTA DE REQUERIMIENTOS NO FUNCIONALES** | |
| **Código** | **Descripción** |
| **RNF01** | El sistema debe implementar controles de seguridad para asegurar la confidencialidad, integridad y disponibilidad de la información. |
| **RNF02** | El sistema debe ser escalable para manejar un aumento en la cantidad de datos y usuarios sin pérdida de rendimiento. |
| **RNF03** | El sistema debe ser intuitivo y fácil de usar para usuarios con diferentes niveles de experiencia. |
| **RNF04** | El sistema debe estar disponible al menos el 90% del tiempo durante el horario laboral. |
| **RNF05** | El sistema debe ser capaz de integrarse con otras aplicaciones de la organización, como SAGU, CISCO, CICA, RRHH. |
| **RNF06** | El sistema debe ser fácil de mantener, con actualizaciones y soporte técnico disponibles. |
| **RNF07** | El sistema debe ser accesible desde diferentes dispositivos, incluyendo móviles y tablets. |
| **RNF08** | El sistema debe ofrecer un rendimiento óptimo, con tiempos de respuesta rápidos y eficientes. |
| **RNF09** | El sistema debe asegurar la confidencialidad de la información mediante controles de acceso y cifrado. |
| **RNF10** | El sistema debe cumplir con los estándares de accesibilidad web, asegurando que personas con discapacidades puedan acceder al sistema sin problemas. |
| **RNF11** | El sistema debe registrar de forma automática todas las acciones de los usuarios para facilitar la trazabilidad de las mismas, para lo cual manejara un historial de modificaciones y accesos. |