**sg-SEG01 - analisis fUNCIONAL**

# DIAGNOSTICO RESUMEN

|  |  |
| --- | --- |
| **ID del Requerimiento** | SG-SEG01 |
| **Título del Requerimiento** | **Seguridad – Control de Acceso Basado en Roles en el Sistema Gestor** |
| **Área de Negocios** | Contabilidad Nacional |
| **Escenario de Negocio** | Sistema Gestor – Seguridad |
| **Elaborado por** | Gabriel García |
| **Fecha** | 02 de Julio de 2015 |

# TABLA DE CONTENIDO

[DIAGNOSTICO RESUMEN 1](#_Toc423694698)

[TABLA DE CONTENIDO 2](#_Toc423694699)

[REQUERIMIENTOS 3](#_Toc423694700)

[1. Objetivo 3](#_Toc423694701)

[2. Alcance 3](#_Toc423694702)

[3. Aspectos relevantes 3](#_Toc423694703)

[DESCRIPCION DETALLADA DE LA ESPECIFICACION FUNCIONAL 5](#_Toc423694704)

[1. Gestión de Objetos del Sistema. 6](#_Toc423694705)

[2. Gestión de Roles. 6](#_Toc423694706)

[3. Gestión de Permisos por Rol. 6](#_Toc423694707)

[4. Gestión de Usuarios. 7](#_Toc423694708)

[5. Gestión de Roles por Usuario. 7](#_Toc423694709)

[6. Consulta Bitácora de Seguridad. 7](#_Toc423694710)

[7. Gestión de Politicas de Seguridad. 8](#_Toc423694711)

[INTERFACES DE USUARIO 10](#_Toc423694712)

[APROBACIÓN 10](#_Toc423694713)

# REQUERIMIENTOS

|  |
| --- |
| **Objetivo, Alcance y Aspectos Relevantes del Requerimiento** |
| Objetivo El presente documento tiene como objetivo establecer los lineamientos generales de Seguridad a nivel de sistema de información que serán desarrollados en el Sistema Gestor. Alcance El Modelo de Seguridad a nivel de Sistema de Información se encarga de dos aspectos importantes, la manera en que se otorgan o se restringen derechos de acceso a cada funcionalidad del sistema y mostrar la forma en que se consulta las pistas de auditoría que muestran la información correspondiente a los cambios sensibles que ha tenido cada tabla o estructura de información.  Este módulo deberá incluir siete componentes:   * Gestión de Objetos del Sistema * Gestión de Roles * Gestión de Permisos por Rol * Gestión de Usuarios * Gestión de Roles por Usuario * Consulta de Bitácora de Seguridad * Gestión de Políticas de Seguridad  Aspectos relevantes Para el diseño del Sistema Gestor se ha seleccionado el modelo RBAC para poder establecer un mecanismo de seguridad eficiente, basado en Roles o Perfiles de usuarios. En una organización un rol puede entenderse como las funciones que puede ejecutar cada puesto o perfil de puesto, por este motivo, los permisos para ejecutar operaciones se asignan a los roles y no directamente a los usuarios, sino que los usuarios adquieren los permisos a través de los roles que tienen asignados. Esto facilita la administración de la seguridad, al no tener la necesidad de asignar usuario por usuario cada permiso que requiera, sino que a los usuarios simplemente se les asignan los roles requeridos para cumplir con sus funciones.   * 1. Definiciones * SG: Siglas utilizadas para referirse al Sistema Gestor. * Role: Rol o Perfil de usuario. * Superusuario: Usuario que puede ejecutar todas las funcionalidades del sistema y manipular todos los formularios e información registrada. * RBAC: Control de Acceso Basado en Roles ó “Role Based Access Control” |

|  |  |
| --- | --- |
| **Resumen de los Resultados arrojados del Análisis** | |
| **Causas del Problema y/o Inconsistencia** | **Área del Ajuste** |
| Los avances tecnológicos en los Sistemas de Información han permitido a las organizaciones tener información de una manera rápida y eficiente lo que permite apoyar la toma de decisiones en todos los niveles, pero principalmente los gerenciales, sin embargo, al ser la información uno de los activos más valiosos de toda organización, es necesario que existan mecanismos que permitan la confidencialidad, disponibilidad e integridad de la misma. |  |

# DESCRIPCION DETALLADA DE LA ESPECIFICACION FUNCIONAL

|  |
| --- |
| **Diagrama de los Procesos Relacionados** |
| Diagrama 1. Modelo de Entidad/Relación Seguridad |
| **Descripción Funcional de los Procesos Relacionados con el Requerimiento y/o Necesidad** |
| Los elementos básicos para el funcionamiento del modelo RBAC son: Gestión de Objetos del Sistema. Para poder administrar los permisos en un sistema de información es indispensable que el mismo cuente con un repositorio de objetos. En el Sistema Gestor los objetos se pueden clasificar en: Menús, Opciones de Menú, Pantallas, Campos, Botones y Otros. Estos objetos por lo general se agrupan en los módulos de la solución para facilitar su gestión. Gestión de Roles. El paso siguiente consiste en identificar los distintos Roles o Perfiles de los usuarios que usarán el sistema, por ejemplo para cada módulo puede existir un Perfil de Administrador del Módulo, el cual por lo general es el encargado de Gestionar los parámetros del módulo, además en cada módulo pueden existir roles de usuarios operativos, estos usuarios serán los que se encarguen de utilizar el sistema para incluir transacciones o movimientos que consisten en las operaciones básicas funcionales de cada módulo. Gestión de Permisos por Rol. Una vez identificados los objetos del sistema y todos los roles o perfiles de los usuarios, se debe delimitar los permisos que cada rol tendrá acceso dentro del Sistema, por lo general se utiliza la siguiente Matriz para delimitar los permisos:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Roles** | | **Rol 1** | **Rol 2** | **Rol N** | | **Objetos** | | | **Módulo 1** | **Pantalla 1** | C + I + M + B | C | C + M | | **Pantalla 2** | C + I | C | C + I | | **Pantalla…** |  | C |  | | **Pantalla N** | C | C | C | | **Módulo 2** | **Pantalla 1** | C | C + I + M + B |  | | **Pantalla 2** | C | C |  | | **Pantalla…** |  |  | C + M | | **Pantalla N** | C |  | C + I | | **Módulo N** | **Pantalla 1** | C + I + M + B | C + M | C + I + M + B | | **Pantalla 2** | C + M | C + I | C | | **Pantalla…** | C | C | C | | **Pantalla N** | C + I | C + I + M + B | C + M |   Tabla 1. Permisos por rol  Donde: C = Consultar, I = Insertar, M = Modificar, B = Borrar. Gestión de Usuarios. Para garantizar la trazabilidad de los cambios en los sistemas de información modernos, así como garantizar que la información sea manipulada solamente por las personas cuyo perfil lo permita, es necesario que los sistemas permitan gestionar los usuarios de la aplicación, son tareas normales dentro de esta gestión la creación de nuevos usuarios, la inactivación de usuarios, la generación de contraseñas, etc. Gestión de Roles por Usuario. Una vez creados los usuarios, el último paso de la gestión es indicar para cada uno de ellos cuáles son los roles o perfiles del aplicativo asignados, al asociar los roles a los usuarios el sistema sabe cuáles son los permisos que cada usuario posee, no se recomienda que existan usuarios sin roles, pero es probable en algunas circunstancias que un usuario posea más de un rol, tampoco es recomendable que existan usuarios que tengan todos los roles de manera que se conviertan en “superusuarios” del aplicativo. Consulta Bitácora de Seguridad. En sistemas de información modernos, es indispensable contar con un mecanismo que permita rastrear las acciones críticas en el sistema, para poder determinar qué usuario y en qué momento ejecutó un proceso o cambió algún dato. En el SG se recomienda tener dos mecanismos de rastreo:   * 1. Rastreo a nivel de registro (Tabla).   Este tipo de rastreo permite determinar en cada estructura de almacenamiento o tabla cuál fue el usuario que creó o insertó el registro y a qué hora del día, así como el último usuario que modificó el registro y el momento del día en que lo modificó. Es un mecanismo básico que no muestra información detallada del cambio realizado, pero permite dar una pista sobre el origen de la información.   * 1. Rastreo en tabla de bitácora de auditoría.   Este mecanismo consiste en guardar en una tabla de bitácora aquellas acciones sensibles o críticas que hayan realizado los usuarios, la tabla de bitácora explicará detalladamente cuáles fueron los cambios o acciones que el usuario realizó. Este es un mecanismo más robusto y complejo, con la desventaja que su utilización constante puede ocasionar la reducción del desempeño del sistema, por lo tanto se recomienda que solamente las acciones críticas se registren en la tabla de auditoría.  Los elementos mínimos que una tabla de auditoría debe tener son: Fecha de ejecución (llegando incluso a nivel de segundo del día), usuario del sistema que realizó la acción o cambio, objeto o pantalla donde se originó la acción/cambio, dirección IP donde se originó la acción/cambio, nombre o identificador de la acción/cambio, y por último una explicación detallada de lo sucedido.  Con respecto al histórico de la bitácora, la misma se debe poder parametrizar para evitar así un crecimiento exponencial de los datos que repercuta en el funcionamiento de la aplicación. Por lo tanto se creará una política de seguridad en la cual el administrador indique el máximo de antigüedad de los datos para ser borrados de esta bitácora automáticamente, antes de ser borrados serán transferidos a otra estructura de manera que la información no se pierda. Gestión de Políticas de Seguridad. Es posible que a nivel de aplicación se puedan definir o parametrizar algunas políticas de seguridad como por ejemplo:   * 1. Complejidad de contraseñas:   Indica qué tan compleja debe ser una contraseña, incluyendo aspectos como tamaño mínimo, cantidad de letras, caracteres especiales y números mínima, no permitir el mismo usuario en la contraseña, restricción de palabras básicas en las claves (password, admin, y otros).   * 1. Reglas de reusabilidad.   Si se debe permitir o no reutilizar algunas contraseñas utilizadas anteriormente por el mismo usuario, estableciendo un límite adecuado, por ejemplo: no permitir reutilizar ninguna de las últimas 5 contraseñas.   * 1. Tiempo ocioso de sesión.   Establecer un máximo de tiempo ocioso por usuario, si el sistema tiene una sesión activa pero no se está utilizando en los últimos minutos, el sistema podría eventualmente terminar o desconectar una sesión automáticamente.   * 1. Cantidad de intentos fallidos de inicio de sesión.   Establecer un máximo de intentos fallidos para iniciar la sesión, al cumplir este máximo el usuario automáticamente se bloqueará, lo que impedirá al usuario iniciar sesión aún cuando haya recordado su contraseña.   * 1. Tiempo de bloqueo de sesión automático:   Permitir establecer un tiempo prudencial en que se bloquee la contraseña después de que el usuario intentó hacer sesión en distintas ocasiones y se cumplió la política anterior.  Inicialmente este tiempo tiene una parametrización indefinida para que haya un proceso de validación donde el usuario solicite el desbloqueo de la cuenta al Administrador de la aplicación.   * 1. Tiempo máximo de vigencia de la contraseña:   Establece un límite de días o meses, cumplido este límite se muestra al usuario un mensaje para obligarlo a modificar su contraseña.   * 1. Cantidad máxima de sesiones por usuario:   Establece un límite sesiones por usuario, por ejemplo, si el sistema detecta que el usuario tiene una sesión activa del usuario Luis Pérez, y Luis Pérez intenta ingresar nuevamente al sistema desde otro equipo, el sistema podría eventualmente impedirlo porque ya se encuentra una sesión activa con este usuario.   * 1. Antigüedad para conservar históricos en Bitácora:   Establece un tiempo prudencial para conservar los registros de bitácora, superado este tiempo se procederá a borrar automáticamente los registros cuya antigüedad exceda lo indicado por este parámetro, antes de ser borrados se trasladarán a otra estructura de manera que sea factible recuperar los datos borrados. |
| **Reglas y Normativas del Negocio a Considerar** |
| El Sistema Gestor estará disponible para dos grandes grupos de usuarios, para funcionarios de Gobierno, ya sea del Ministerio de Hacienda, Unidades Primarias de Registro u otros Ministerios o Entidades de Gobierno, quienes se autenticarán en el Sistema Gestor por medio de su firma digital y para todos los ciudadanos costarricenses por internet, quienes utilizarán el módulo de Captura de Ingresos para crear nuevos formularios de pago; por este motivo, debe existir un modelo de autenticación híbrido que permita autenticar a los ciudadanos por medio de un usuario y contraseña y a los funcionarios de Gobierno por medio de firma digital. Los ciudadanos que posean firma digital incluso pueden realizar el pago directamente en el sistema, si por el contrario el ciudadano no posee firma digital, puede imprimir su formulario de pago y presentarse con el formulario impreso a cancelar el monto correspondiente en algún banco o Unidad Primaria de Registro.  A continuación se listan los módulos y las áreas que utilizarán el Sistema Gestor.   |  |  | | --- | --- | | Módulo | Área | | Consolidación | Contabilidad Nacional  Unidades Primarias de Registro | | Captura de Ingresos | Contabilidad Nacional  Público en General  Tesorería Nacional  Unidades Primarias de Registro | | Contingentes | Unidades Primarias de Registro  Unidad Patrimonial  Unidad Asesoría | | Revelación de Notas | Unidades Primarias de Registro  Unidad de Análisis Contable  Unidad de Consolidación de Cifras | | Deuda Externa | Contabilidad Nacional  Crédito Público  Unidades Primarias de Registro | | Deuda Interna | Contabilidad Nacional  Tesorería Nacional  Unidades Primarias de Registro | |

# INTERFACES DE USUARIO

|  |
| --- |
| **Detalles de las vistas a desarrollar** |
| No aplica. |

# APROBACIÓN

|  |  |
| --- | --- |
| **Aprobaciones/Firmas** | |
| Funcional SG  Jeannette Solano |  |
| Funcional SG  Diego Lopez |  |
| Funcional SG  Karina Ledezma |  |
| Consultor PwC  Gabriel García Granados |  |