DEPARTAMENTO NACIONAL DE PLANEACION

OFICINA DE CONTROL INTERNO

EVALUACION AL SISTEMA DE INFORMACIÓN GESPROY - SGR

INFORME DEFINITIVO

BOGOTA, DICIEMBRE DE 2014

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Oficina de Control Interno, en desarrollo del plan de operativo aprobado para la vigencia 2014 programó efectuar la evaluación al sistema de información GESPROY - SGR, actividad que se desarrolló como parte de sus funciones en el marco de la Ley 87 de 1993.

La evaluación estuvo orientada al fortalecimiento del Control Interno como mecanismo de apoyo al logro de los objetivos propuestos por el área que coordina el sistema de información, objeto de la evaluación en cumplimiento de lo establecido en el artículo 2 de la Ley 87 de 1993, el cual establece la función de la Oficina de Control Interno en cuanto a planear, dirigir y organizar, la verificación.

Esta evaluación se realizó con base en las normas de auditoría interna de general aceptación, las cuales incluyeron planeación de la evaluación, ejecución del trabajo y generación de informe. Para la ejecución de la evaluación se emplearon, entre otras, técnicas de muestreo que se aplicaron a las operaciones, registros y controles asociados al Sistema de Información.

Para el logro de los objetivos propuestos fue de vital importancia la participación de los responsables de administrar y coordinar el Sistema de Información, así como el suministro de la información soporte y complementaria generada a partir del funcionamiento del mismo.

El proceso de evaluación involucró la solicitud, análisis y verificación de la información relacionada con la seguridad del sistema GESPROY de acuerdo con el alcance establecido en la presente evaluación; adicionalmente se establece la presentación de resultados, una vez sean analizados con el(los) responsable(s) del sistema, con los que se pretende contribuir al mejoramiento continuo de éste.

2. OBJETIVO GENERAL

Verificar en el Sistema Gesproy – SGR, en el marco del proceso de "Gestion de Seguridad de la Información", la aplicación de los criterios establecidos en el Manual de Seguridad de la Información para proteger los activos de información, el control de acceso y la gestión de incidentes, así como las Políticas de Seguridad para Aplicativos y Portales Web Informáticos, de tal forma que se pueda establecer su aplicación en la administración de los riesgos de seguridad de la información y proponer oportunidades para la mejora como producto de la evaluación.

3. OBJETIVOS ESPECÍFICOS

Verificar y analizar la aplicación de los criterios definidos por la Entidad en materia de seguridad de la información para la protección de activos de información tecnológica, en el marco del proceso de Seguridad de la Información.

Verificar y analizar la gestión de incidentes de seguridad de la información presentados durante la vigencia 2014.

Identificar y analizar la gestión de riesgos realizada durante la vigencia 2014.

Analizar e Identificar oportunidades para la mejora, producto de la evaluación realizada.

4. MARCO LEGAL

Para la evaluación a realizar se tuvo en cuenta entre otros, los siguientes aspectos legales que regulan o pueden aportar buenas prácticas para el funcionamiento del Sistema de Información GESPROY – SGR:

- Ley 1530 de 2012 (Art. 9,28 y 100)
- Decreto 1832 de 2012
- Decreto 414 de 2013
- Resolución 340 de 2013 del DNP
- Circular No. 0062 de 2013
- Proceso de Gestión de Seguridad de la Información del SGC vigente.
- Manual y Políticas de Seguridad de la Información del Departamento Nacional de Planeación.
- Norma ISO 27000 – 27001 y 27005. Marco de referencia de estándares internacionales para una mejor práctica en la Seguridad de la Información.

5. ALCANCE

La evaluación se realizó al Sistema de Información Gesproy - SGR teniendo como marco de evaluación las políticas definidas en el Manual de Seguridad de la Información, las políticas de Seguridad Informática definidas por la OI para aplicativos y portales web y la Información recopilada por medio de la presente auditoría, para el periodo establecido entre el primero (1) de enero al (31) de Octubre de 2014, con el fin de establecer su aplicación en la administración de los riesgos de seguridad de la información y proponer oportunidades para la mejora como producto de la evaluación.

6. METODOLOGÍA

La Oficina de Control Interno tuvo como marco de referencia las normas de auditoria de general aceptación (NAGA) sobre las cuales orientó su labor con el propósito de determinar el estado del sistema de control interno en los aspectos definidos en el alcance de la evaluación.

Para el análisis de los aspectos antes mencionados se revisó la información suministrada por la Coordinación del Sistema de Información GESPROY -SGR, para lo cual se emplearon diferentes medios como: solicitud y recopilación de información; verificación, confrontación y análisis de la información obtenida; realización de entrevistas a los funcionarios del área respectiva; validación técnica de las políticas de seguridad en el aplicativo las cuales están alineados con lo especificado en el numeral 11.1 “Requisitos del negocio para el control del acceso”, 11.2 “Gestión del acceso de usuarios” y 11.3 “Responsabilidades de los usuarios” de la norma NTC-ISO/IEC 27002:2005.

Como complemento de la metodología se adelantaron las siguientes actividades:

1. Revisión y análisis de la información suministrada por la coordinación o líderes funcionales del Sistema de Información.

2. Revisión del sistema de información GESPROY – SGR identificando y determinando aspectos de cumplimiento de las políticas de seguridad de la información definidas en el alcance del plan de trabajo.
3. Análisis de los mecanismos empleados para la gestión de incidentes de seguridad de la información.
4. Análisis de la gestión de riesgos de seguridad de la información.
5. Identificación de fortalezas, hallazgos y oportunidades de mejora una vez revisada y analizada la documentación del Sistema definida en el alcance de la evaluación.
6. Consultas a la base de datos del aplicativo GESPROY-SGR para evidenciar aspectos relacionados con la auditoría del aplicativo y con la gestión de usuarios y perfiles.

7. DESCRIPCIÓN DEL SISTEMA DE INFORMACIÓN GESPROY - SGR

Es el sistema que apoya las actividades de seguimiento, control y ejecución de proyectos financiados con recursos del Sistema General de Regalías (SGR); en éste, los entes ejecutores se encargan de reportar la información correspondiente a la programación, contratación y ejecución de los proyectos financiados con recursos del SGR.

El aplicativo GESPROY-SGR actualmente está activo y es utilizado por mil ciento treinta y dos (1132) entidades las cuales tienen usuario, de las anteriores entidades se tienen tres mil cuarenta y dos (3042) cuentas de usuarios activas y, dos mil setecientos setenta y seis (2776) proyectos migrados de SUIFP (aprobados) desde el 01 de enero al 31 de octubre del 2014 (información extraída del correo enviado por la dependencia –aaparicio@dnp.gov.co- el 16 de diciembre de 2014).

La interoperabilidad de Gesproy SGR, se observa en la interface que tiene éste Sistema con varios aplicativos del Sistema General de Regalías así:

Aplicativo Cuentas SGR, del cual se extrae la relación de pagos registrados en la cuenta maestra del proyecto.

Aplicativo SUIFP –SGR, Gesproy carga, mediante un proceso de sincronización de datos desde el Banco de Proyectos FUIFP – SGR, la información básica de formulación del proyecto.

Mapa Regalías, se genera interface con éste aplicativo con el fin de proporcionar registro fotográfico del avance del proyecto e información de avance financiero y físico del proyecto.

8. EJECUCIÓN DE LA EVALUACIÓN

8.1 ANALISIS DE LA APLICACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

8.1.1 "Gestión de Activos de Información" frente al Sistema Gesproy –SGR.

Pruebas

Se efectuó el análisis de la aplicación de las políticas de Gestión de Activos de Información sobre el desarrollo realizado del Sistema de Información, analizando la arquitectura del sistema, su documentación, el empleo de los repositorios de información para la conservación de éstos registros y el control que se tiene sobre los mismos por parte de los funcionarios o contratistas que forman parte del equipo desarrollador del Sistema de Información.

Frente a la arquitectura del Sistema, de acuerdo con el Manual Técnico, se tiene que Gesproy SGR usa una arquitectura de tres capas, cada uno de los cuales ofrece los servicios de persistencia, reglas del negocio y servicio de Interfaz gráfica para el usuario (GUI).

Tiene implementado un patrón MVC (modelo, vista y controlador para garantizar la independencia de cada uno de los módulos), mediante el uso de clientes delgados donde cada uno de ellos tiene la presentación por un navegador; sobre el tema particular de arquitectura no se tienen observaciones en la presente evaluación.

Documentación del Sistema de Información y Repositorios de Información

La documentación del Sistema de Información Gesproy SGR se encuentra en el repositorio de información Team Foundation, en el cual se conservan las versiones finales de los documentos del sistema, entre ellos, el código fuente, los manuales de usuarios y técnico, el plan de acción del Sistema de Información y la documentación relacionada con la administración de riesgos como lo es el mapa de riesgos, plan de contingencia y políticas de seguridad de la información.

Durante la revisión de la documentación mencionada en reunión sostenida el día 16 de diciembre de 2014, se observó que la última versión del Manual de Usuario que se tenía en el repositorio correspondía a la V 2.8 del 6 de noviembre de 2014, de igual forma la versión del anexo que hace parte constitutiva del manual corresponde a la versión 2.7 del 22 de Octubre de 2014, en contraste con esta situación, la Versión del Manual de Usuario observada en la página web del Sistema General de Regalías corresponde a la Versión 2.9 del 9 de diciembre de 2014, sin embargo durante la evaluación realizada el equipo de tecnología corrigió esta situación.

De otra parte se revisó el plan de acción del Sistema de Información que fue reportado para la vigencia 2014; frente al plan se revisó el control aplicado para verificar su cumplimiento, encontrando que el equipo de tecnología de la Dirección de Vigilancia de las Regalías además de realizar un seguimiento al plan de acción, lleva un cronograma de trabajo articulado con el plan de acción del Sistema, con el cual se efectúa seguimiento semanal al cumplimiento de las actividades definidas para la vigencia. Es importante resaltar que el alcance del cronograma es mayor al del plan de acción de Gesproy SGR, ya que en él se agrupa para seguimiento, no sólo lo relacionado con el Sistema de Información sino todas las actividades realizadas por el equipo frente a los aplicativos de la Dirección de Vigilancia de las Regalías (DVR).

En entrevista realizada a los responsables del seguimiento semanal del Cronograma de Trabajo, se pudo establecer que si bien se tiene implementada la herramienta de seguimiento, el plan de acción se encontró desactualizado frente a las fechas de finalización de algunas de las actividades o requerimientos que habían sido reprogramadas en el cronograma de trabajo, como fue el caso de las actividades No. 19, 27, 28, 31, 35 del plan de acción; sin embargo después de finalizada la evaluación del plan por parte de la Oficina de Control Interno OCI, el equipo de tecnología remitió el documento actualizado.

Frente a la estructura del plan de acción y del cronograma de trabajo, se observó que algunas columnas importantes para el seguimiento no tienen la misma denominación en ambos documentos y puede generar inexactitud en el seguimiento o la estimación de fechas de las actividades; es el caso de las siguientes columnas:

Según Cronograma de Trabajo

FECHA ENTREGA PARA PRUEBAS GT	FECHA ENTREGA A USUARIOS	TECNOLOGÍA FECHA PRODUCCION

Según Plan de Acción:

TECNOLOGÍA FECHA ENTREGA DESARROLLO	TECNOLOGÍA FECHA ENTREGA PRUEBAS	TECNOLOGÍA FECHA PRODUCCION

En el caso anterior, las columnas no se denominan de igual forma y pueden generar ambigüedad, como es el caso de las columnas “Fechas de entrega de desarrollo” y “Fecha de entrega a usuarios”.

Tener en cuenta lo anterior puede contribuir con la mejora del seguimiento realizado en el cronograma y en el caso particular del plan de acción del aplicativo Gesproy SGR, de tal forma que pueda evidenciarse con mayor precisión la articulación existente entre estos dos documentos o del plan de acción de cualquier otro aplicativo de la DVR.

Una vez realizada la verificación en sitio de los documentos que soportan el plan de acción de la vigencia 2014 y teniendo en cuenta las situaciones presentadas durante la evaluación se plantea la siguiente oportunidad que contribuye con el manejo documental del Sistema de Información:

Oportunidad de Mejora No. 1

Durante la auditoría realizada a la documentación del Sistema de Información, se observaron debilidades en el control de las versiones de los documentos: Manual de usuarios, anexo del manual de usuarios y plan de acción del Sistema de Información en el repositorio de información Team Foundation Server, ya que durante el proceso de auditoría fueron encontradas en el repositorio de

información versiones anteriores a los documentos vigentes, si bien la situación fue corregida durante la evaluación realizada por la Oficina de Control Interno, esto genera el riesgo de inexactitud de información en la documentación del sistema de información, lo que podría conllevar a pérdida de credibilidad y confianza en la administración de la misma.

Recomendación

Generar un mecanismo de control que permita una revisión continua e integral a la documentación del Sistema de Información para asegurar que las versiones vigentes y pertinentes de los documentos se encuentran disponibles en una única base de información.

De acuerdo con la respuesta realizada por el Grupo de Tecnologías de la Información de la DVR mediante Rad. 20144400146223 se informa:

> Se procederá a generar un mecanismo de control que permita una revisión continua e integral a la documentación del Sistema de Información para asegurar que las versiones vigentes y pertinentes de los documentos se encuentran disponibles en una única base de información.

Consideraciones de la Oficina de Control Interno: Teniendo en cuenta que se procederá a implementar un mecanismo de control sobre la actualización de los documentos del Sistema de Información, se recomienda documentar las acciones que sean orientadas al control y actualización de los documentos del Sistema de Información.

8.1. 2 Autenticación y autorización

La autentificación es el proceso de detectar y comprobar la identidad de una entidad de seguridad examinando las credenciales del usuario y validando esas credenciales contra alguna autoridad. La información obtenida durante la autenticación puede ser utilizada directamente por el código. Como la plataforma del DNP es generalmente Microsoft, también se puede usar la seguridad basada en roles de .NET Framework para autenticar al usuario actual y determinar si esa entidad de seguridad puede obtener acceso al código.

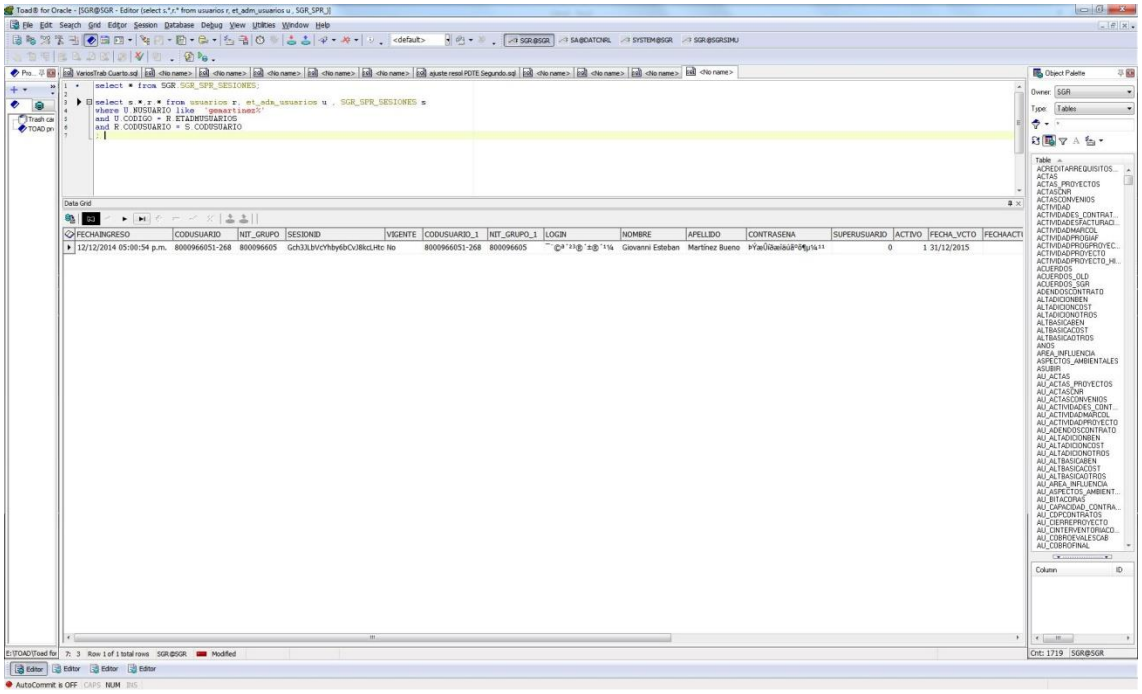
Actualmente se utiliza una gran variedad de mecanismos de autenticación, pudiéndose utilizar muchos de ellos con la seguridad basada en roles de .NET Framework. Algunos de los mecanismos de

autenticación que se utilizan más habitualmente son la autenticación básica, implícita, Passport y de sistema operativo (como NTLM o Kerberos), o los mecanismos definidos por la aplicación.
La autorización es el proceso de determinar si se permite a una entidad de seguridad realizar una acción solicitada. La autorización tiene lugar después de la autenticación y utiliza información relativa a la identidad y roles de la entidad de seguridad para determinar a qué recursos puede tener acceso la entidad de seguridad.
La Oficina de Informática ha establecido una política respecto al proceso de autenticación y autorización la cual dice: "Proceso de autenticación y autorización, garantizando autenticación única - una sola vez- y único usuario (Single Sign-On). Para el caso de usuarios internos DNP debe ser contra Directorio Activo el proceso de autenticación y en cada aplicación el proceso de autorización".

Pruebas

- Se verificó que el usuario de inicio de sesión en el dominio en la Intranet del DNP es el mismo con el que se inicia sesión en GESPROY.
- Se verificó que la contraseña del usuario del dominio de la intranet del DNP es la misma cuando se hace la autenticación en GESPROY.
- Se realizó cambio de contraseña en el dominio de la intranet del DNP y cuando se realizó el inicio de sesión en GESPROY, se reflejó el cambio de credenciales cuando se hizo la autenticación.
- Se revisaron en la tabla que soporta los inicios de sesión y el tiempo de las sesiones activas, el manejo del método de autenticación. Autenticación contra Directorio Activo (usuarios internos: DNP) y autenticación contra Base de Datos (usuarios externos: Entidades Ejecutoras).

Se concluye que la solución cumple con la política 1 de seguridad para aplicativos, en donde hay solo una credencial para el usuario del dominio y el de GESPROY; adicionalmente, se verificó en la tabla de auditoría de inicios de sesión la huella que se almacena para usuarios internos y para usuarios externos, evidenciando el diferente método para cada uno de estos tipos de usuarios; para usuario interno el mecanismo de autenticación implementa integración con el Directorio Activo, mientras que para usuarios externos solo contra base de datos (ver imagen a continuación tomando como muestra el usuario gemartinez):



8.1.3 Administración de usuarios y perfiles

La administración de usuarios y perfiles es un aspecto fundamental en la construcción de soluciones en donde se requiere establecer ciertos niveles de acceso a la información según su grado de privacidad y confidencialidad.

La Oficina de Informática ha establecido una política para el manejo de usuarios y roles así: "Administración de usuarios y perfiles, donde los perfiles se conforman de roles y permisos."

Pruebas

- La existencia de perfiles de usuario de acuerdo al nivel de acceso y a la clasificación de las operaciones realizadas en GESPROY.
- La existencia de un mecanismo de asignación de perfiles a cada uno de los usuarios de GESPROY.

Se verificó que en las tablas "USUARIOS, PERFILES_USUARIOS, ET_ADM_USUARIOS, ET_ADM_PERFILES y DT_ADM_PERSONAS" se gestiona la información y forma parte del

mecanismo para el otorgamiento de permisos, de acceso y de autorización del aplicativo. Lo anterior da cumplimiento a la política mencionada y por lo tanto no se tienen observaciones al respecto.

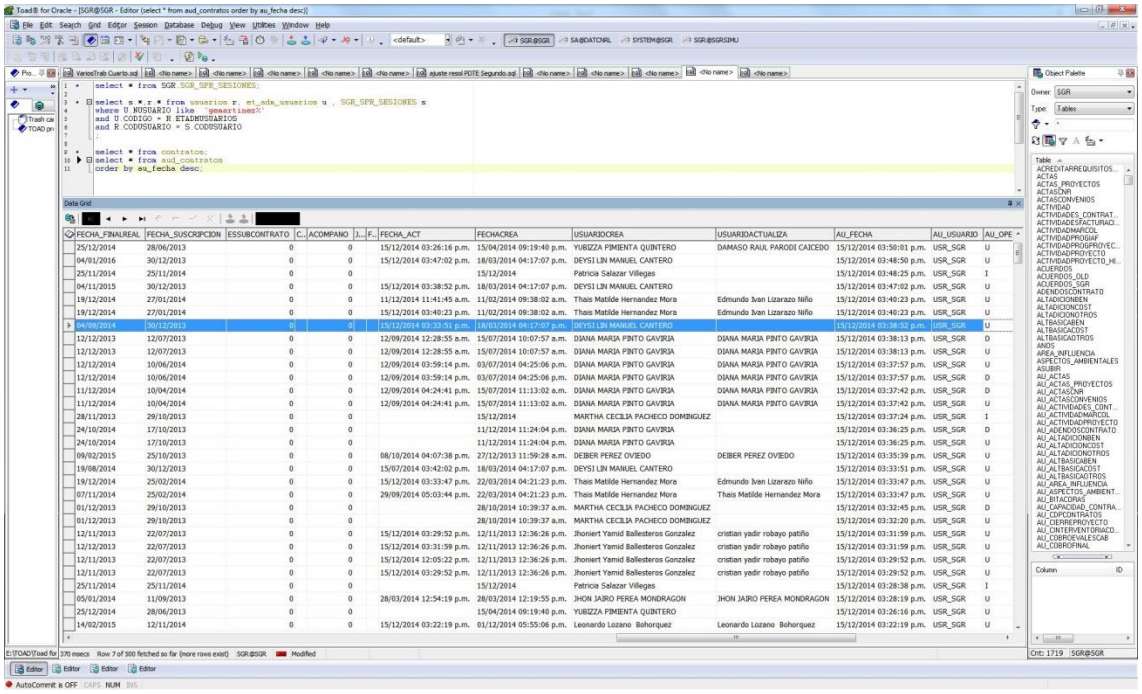
8.1.4 Auditoría

En aplicativos y portales web informáticos se pueden implementar mecanismos de auditoría en las diferentes capas de las soluciones de software, bajo un alto grado de abstracción, las auditorías se implementan en la capa de persistencia -programadas manualmente o utilizando la funcionalidad del motor de bases de datos -, y/o en las capas de negocio y presentación.
La Oficina de Informática ha establecido una política sobre el manejo de auditorías en las soluciones de software que se construyan para el DNP, dicha política dice: “Deben incluir auditoría para la aplicación, es decir, todos los accesos de ingreso y transacciones deben ser monitoreados y registrados a fin de generar un rastro de referencia”.

Pruebas

- La existencia de mecanismos de auditoría para el acceso al aplicativo GESPROY.
- La existencia de mecanismos de auditoría para la gestión de información por medio del aplicativo GESPROY.

Como resultados de la pruebas se verificó que las auditorías están implementadas en las capas de presentación y de negocio. Se registra los inicios de sesión de los usuarios y dicho registro es insumo para el mecanismo de expiración de sesión desatendida; igualmente, para la auditoría de operaciones de usuario, se registran datos como la identificación del usuario, la fecha del evento, el tipo de operación (inserción de registro, modificación de registro, eliminación de registro). Como evidencia se muestra una imagen de una consulta realizada a las tablas de auditoría sobre las operaciones que realizan los usuarios:



8.1.5 Comunicaciones seguras

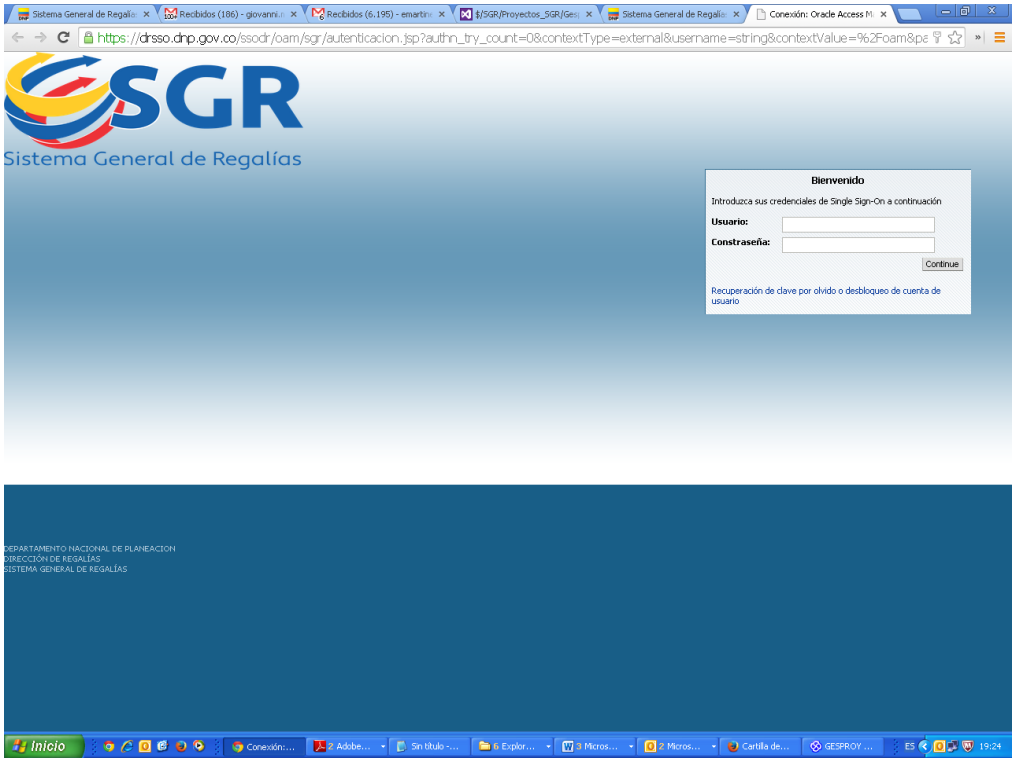
Teniendo en cuenta que la información se puede encontrar en alguno de los siguientes estados "almacenada", "en procesamiento" o "siendo transmitida", y dado que la Oficina de Informática del DNP ha establecido una política que respalde la seguridad de la información cuando está transmitiéndose entonces se hace necesario dar cumplimiento a la misma por los riesgos de seguridad informática existentes relacionados con el robo y la manipulación no autorizada de la información.

La política que la Oficina de Informática ha definido para las comunicaciones seguras es: "Comunicaciones seguras a fin de proteger las transferencias de datos entre componentes y servicios remotos".

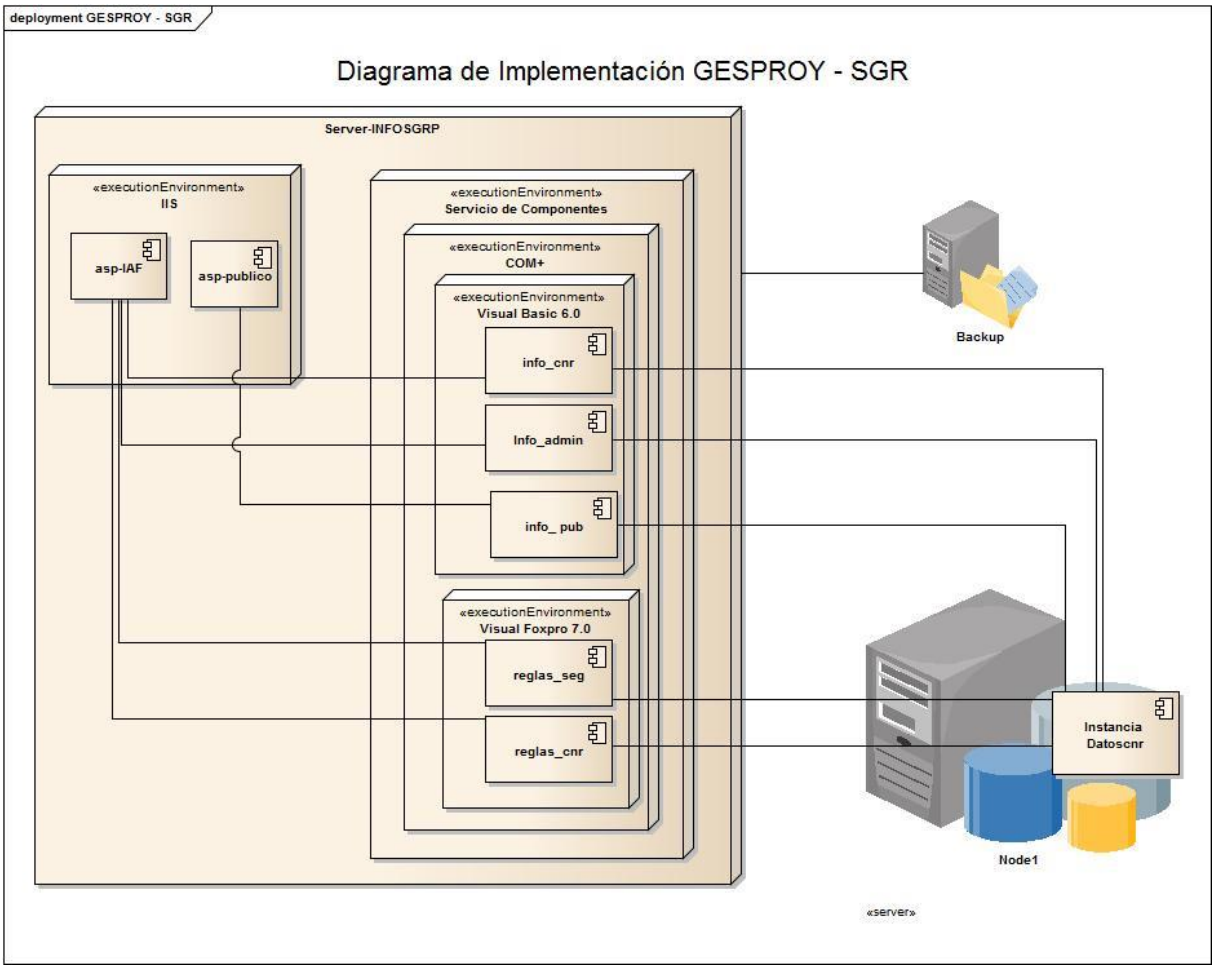
Pruebas

- Se revisaron los protocolos de comunicaciones que GESPROY utiliza iniciando sesión en la aplicación y navegando por los formularios que lo componen.
- Se revisó el diagrama de implementación de GESPROY el cual se encontró en http://vtfsapp:8080/tfs/DR/SGR/_versionControl#path=%24%2FSGR%2FProyectos_SGR%2FGesproy+SGR%2FDise%C3%B1os%2Ftecnico&_a=contents.

Como resultado de las pruebas se verificó que el protocolo empleado para el envío de credenciales en el formulario de inicio de sesión es “HTTPS” el cual es un protocolo que implementa el servicio de cifrado de la información que se transmite por él, como registro se muestra la imagen correspondiente al formulario mencionado:



De acuerdo a la entrevista realizada al grupo GTI-DVR, ellos manifiestan que solo utilizan https como protocolo de seguridad en el caso de uso o funcionalidad de autenticación y que no se utiliza en ningún otro formulario; adicionalmente en el diagrama de implementación de la solución el cual se muestra a continuación, no se visualizan los protocolos de comunicaciones utilizados por la solución tecnológica.



Teniendo en cuenta la respuesta generada al informe preliminar por el Grupo de Tecnologías de la Información de la DVR mediante Rad. 20144400146223 en la que se señala el texto descrito a continuación, el hallazgo No. 1 del Informe Preliminar se ajusta como Oportunidad de Mejora, en consideración a la recomendación realizada por la OI:

> Teniendo en cuenta el literal *d) Comunicaciones seguras a fin de proteger las transferencias de datos entre componentes y servicios remotos* de las "Políticas de seguridad para aplicativos y portales Web informáticos" y soportando que estamos proporcionando seguridad en el login como lo indica la revisión de la OCI, se procedió hacer la consulta a la OI del DNP a razón de obtener el alcance de dicho literal en cuanto a nuestro sistema de información GESPROY-SGR.
>
> Consulta a la Oficina de Informática del DNP:

El aplicativo Gesproy SGR utiliza autenticación segura en el formulario del LOGIN, el cual utiliza protocolo HTTPS dando cumplimiento al literal d) de "Políticas de seguridad para aplicativos y portales Web informáticos" garantizando la confidencialidad de los datos de autenticación del usuario.

Es necesario que para todos los formularios que hacen parte del aplicativo se utilice el protocolo?
Se verificó los lineamientos nuevamente y se entiende que se deberá utilizar SSL siempre que se intercambien datos confidenciales con el usuario como, por ejemplo, cuando se envíen formularios de inicio de sesión o se muestre información financiera personal.

Respuesta de la Oficina de Informática del DNP:
Este protocolo es recomendable usarlo en todos los formularios que transfieran información y que requieran estar autenticados o transfieran datos a los servidores de las aplicaciones, sin embargo su uso asegura al visitante de un sitio web o aplicativo la autenticidad del mismo asegurando que el sitio web es quien dice ser probando la identidad de la empresa y de esta forma crear un sentido de fiabilidad y confianza a quien usa su sitio web.

Con base en lo pronunciado por la Oficina de Informática y teniendo en cuenta que el sistema de información GESPROY-SGR maneja confidencialidad de los datos de autenticación del usuario y que el protocolo es recomendable usarlo, solicitamos a ustedes que el hallazgo sea una oportunidad de mejora. Se adjunta evidencia de la respuesta de la Oficina de informática.

Oportunidad de Mejora No. 2 – Comunicaciones Seguras

Una vez realizadas las pruebas descritas anteriormente, se identificó que solo se utiliza comunicación segura en el formulario de autenticación (inicio de sesión) de la aplicación y no se utilizan comunicaciones seguras en la transmisión de información (datos) en el resto de formularios que componen la solución. Teniendo en cuenta las explicaciones dadas por el GTI-DVR y la OI, quienes aclaran que el cumplimiento de la política de comunicaciones seguras la realizan para datos confidenciales (credenciales del usuario); pero igualmente, teniendo en cuenta que hay cargue de datos en otros formularios, que independiente de su carácter de públicos, se debe asegurar su integridad; la falta de aplicación integral de éstas políticas, genera el riesgo de manipulación de los datos que se están transmitiendo e inexactitud de los datos que se están almacenando en el sistema de información, lo que podría conllevar a pérdida de credibilidad y confianza en la administración del mismo.

Recomendación

Se recomienda a los responsables técnicos incorporar el uso de comunicaciones seguras para todos los formularios (páginas) en que hay cargue de datos y consulta de datos de GESPROY-SGR.

8.1.6 Soporte a Usuarios

El soporte a usuarios del Sistema GESPROY SGR tiene varios canales de comunicación, entre ellos, de acuerdo con el Manual de Usuario "SISTEMA DE GESTIÓN Y MONITOREO A LA EJECUCIÓN DE PROYECTOS GESPROY- SGR", se encuentran para el Sistema de Información dos email y varias líneas telefónicas:

APLICATIVO	EMAIL	TELEFONO	EXTENSIONES
Gesproy SGR	gesproysgr@dnp.gov.co	(1) 381 50 00	4062 – 4063
Cuentas SGR Gesproy SGR	infosgr@dnp.gov.co	(1) 595 43 37 01 8000 94 2626	NA

Como complemento a lo anterior se informó por parte del equipo de Tecnología responsable del Sistema de Información que se tienen otras extensiones disponibles para brindar soporte técnico como lo es la extensión (Tel. 3815000) 4055 y la extensión 3868 que se encuentra re direccionada a la extensión 4062, éstas atendidas por el equipo de soporte técnico compuesto por cuatro consultores.

En cuanto al material de apoyo que soporta las actividades de los usuarios, se tiene disponible en la página web del Sistema General de Regalías, para facilitar la gestión de los usuarios del Sistema y fortalecer su nivel de conocimiento y administración del mismo, una sección denominada "Material complementario Gesproy" con la cual se ponen a disposición del público videos tutoriales que explican la Operación del Sistema de Información en cuanto al ingreso al aplicativo y la operación realizada en cada una de sus secciones constitutivas: Descripción General, Entidad Ejecutora, Cumplimiento de

Requisitos, Fuentes de Financiación, Incorporación Presupuestal, Planeación Cargue de la Planeación Inicial, Gestión Precontractual, Contratos, Aprobación de Información, Alertas del Proyecto, Auditorías Visibles, Indicadores y Avance, Cuentas y Giros.

De otro lado se ha diseñado el documento "Tips para el manejo eficiente de la herramienta" que aclara aspectos relacionados con la gestión de Creación de usuarios Gesproy SGR, Prerrequisitos para visualizar proyectos, Proyectos con ajustes, Últimos ajustes del sistema y Errores comunes de los usuarios. De igual forma en el Sistema de Información se encuentra la sección de mesa de ayuda que brinda a los usuarios la información requerida para su soporte.

Frente al material de apoyo se observa que la Entidad tiene a disposición de los usuarios de Gesproy SGR herramientas para facilitar la gestión de los clientes del Sistema.

Pruebas

Con el fin de verificar el funcionamiento de los canales de soporte a usuario, se adelantó en las fechas: del 12, 15, 16 y 17 de diciembre la revisión del funcionamiento de las líneas telefónicas 3815000 Ext. 4062 – 4063, y las líneas 5954337 y 018000942626, encontrando que para el primer caso las dos extensiones son atendidas por personal de soporte del Sistema de Información Gesproy SGR, mientras que para el caso de la línea 5954337, referenciada en el manual de usuario Versión 2.9 del 9 de diciembre de 2014, que se descarga de la página web del SGR, se encontró deshabilitada para las ocasiones que se marcó con el fin de determinar su funcionamiento, sin observar en la documentación del sistema, descripción alguna que indique restricciones sobre el uso de la línea.

De otra parte se observó al ingresar a Gesproy SGR, en la sección "Mesa de Ayuda", que se tiene a disposición de los usuarios para soporte técnico la línea celular 3186755466, la cual no es mencionada en el manual de usuario y la línea telefónica 5954337, referenciada en el manual de usuario Versión 2.9 que no es mencionada en la sección de la Mesa de Ayuda del Sistema de Información.

En cuanto a los correos electrónicos de soporte, se observó el funcionamiento de los correos electrónicos gesproysgr@dnp.gov.co y infosgr@dnp.gov.co de acuerdo con el registro de respuestas realizadas a las entidades territoriales.

Del análisis realizado a la información de soporte a usuarios surge la siguiente oportunidad de mejora:

Oportunidad de Mejora No. 3

Durante la revisión del Manual de Usuario del Sistema de Información GESPROY SGR "SISTEMA DE GESTIÓN Y MONITOREO A LA EJECUCIÓN DE PROYECTOS GESPROY- SGR" se observó en el numeral 1 "Esquema de Soporte a Usuarios", que la línea telefónica 5954337 no se encuentra en funcionamiento una vez fueron realizadas llamadas en las fechas: 12,15, 16 y 17 de diciembre de 2014, con el fin de evidenciar la prestación del servicio por este canal; lo anterior genera riesgos en la categoría de incumplimiento de compromisos por debilidades en la información de los canales para la prestación del servicio de soporte a usuarios, lo que genera efectos para la Entidad como pérdida de credibilidad y confianza debido a los errores en la información suministrada.

Recomendación

Actualizar el Manual de Usuarios del Sistema de Información Gesproy SGR con las líneas telefónicas vigentes o la inclusión de las restricciones a que haya lugar sobre las mismas.

De acuerdo con la respuesta realizada por el Grupo de Tecnologías de la Información de la DVR mediante Rad. 20144400146223 se informa:

> El manual de usuario del sistema de información GESPROY-SGR, debe contener los medios de atención a usuarios dispuestos por el DNP. El contrato del CALL CENTER supervisado por el DNP que atendía las solicitudes del SGR incluía el número de teléfono y cuenta de correo señalados en la oportunidad de mejora. Dicho contrato, según información suministrada vía telefónica por la anterior supervisora finalizó el pasado mes de julio, teniendo en cuenta que no se nos informó de dicha finalización, en el manual aún reposaba esos datos. Se procedió hacer la actualización.

Consideraciones de la Oficina de Control Interno: Teniendo en cuenta que se procedió a realizar la actualización del Manual de Usuarios y que se efectuó corrección sobre el tema, se recomienda documentar las acciones que sean orientadas al control y actualización de los documentos del Sistema de Información.

8.2 ANÁLISIS DE LA ADMINISTRACIÓN DE RIESGOS

8.2.1 Mapa de Riesgos

Se observó que el aplicativo cuenta con su mapa de riesgos, el cual se encuentra construido de acuerdo con los criterios establecidos en la "Guía para la Administración de Riesgos en Seguridad de la Información" elaborada por la Oficina de Informática (OI); el mapa se encuentra ubicado en el repositorio de información Team Foundation Server y fue elaborado en conjunto entre el equipo técnico del Sistema de Información y personal de la OI.

En entrevista con colaboradores del equipo Coordinador del Sistema de Información Gesproy SGR, se identificaron los riesgos y los controles documentados del mapa de riesgo observando que el mapa tiene documentados cinco riesgos: "Daño a la Información en SGR", "Fuga de Información en SGR", "Hurto de la Información en SGR", "Perdida de Integridad de la Información en SGR" y "No Disponibilidad de la Información en SGR". La identificación de riesgos obedece a las categorías definidas en la "Guía para la Administración de Riesgos en Seguridad de la Información".

Dentro de los controles documentados se encuentran: Token, control de acceso, protocolos de seguridad, plan de contingencia, copias de respaldo, documentación, control de versiones del código fuente, antivirus, políticas de seguridad, monitoreo de servicios, logs de auditoría y campañas de sensibilización.

Los controles encontrados en el mapa de riesgos del Sistema, se encuentran soportados sin embargo se observa una oportunidad para la mejora en cuanto al Plan de Contingencia.

8.2.2 Plan de contingencia

De acuerdo con la información remitida por la dependencia se observó que el Sistema tiene diseñado un plan de contingencia en el numeral 9 “Sistema de Gestión de Proyectos GESPROY –SGR” del documento denominado “Plan de Contingencia de los Aplicativos de la Dirección de Vigilancia de las Regalías”. El documento se compone de las secciones denominadas: Misión del Sistema, Estructura de la Aplicación, interfaces con otras aplicaciones, procesos y productos críticos, información del contacto clave, implementación del plan, todas ellas describen el detalle de las actividades a realizar en contingencia.

Sobre las secciones mencionadas se tienen las siguientes oportunidades de mejora relacionadas con la Estructura de aplicación, la implementación del plan de contingencia y la denominación del equipo responsable del Sistema de Información; en cuanto a las demás secciones del plan de contingencia no se presentan observaciones en el presente informe:

Oportunidad de Mejora No. 4

Durante la revisión del Plan de Contingencia se observó que la sección “Estructura de la Aplicación” hace mención a los proyectos que son financiados con recursos del Fondo Nacional de Regalías o FAEP, lo cual no corresponde al Sistema GESPROY SGR, puesto que su gestión está orientada a los proyectos financiados con recursos del Sistema General de Regalías, adicionalmente el nombre del equipo técnico responsable de éste Sistema de Información que figura en el plan de contingencia no es el mismo con el que se conoce en la Dirección de Vigilancia de las Regalías, ya que en el documento del Plan figura como “Grupo de Sistemas Dirección de Vigilancia de las Regalías” y el equipo recibe el nombre de Grupo de Tecnologías de la Información de la Dirección de Vigilancia de las Regalías. Lo anterior, genera el riesgo de inexactitud de información en la documentación del sistema de información, lo que podría conllevar a pérdida de credibilidad y confianza en la administración de la misma.

Recomendación

Se sugiere adelantar la revisión del documento del Plan de Contingencia de manera integral para actualizar aquella información que no corresponde actualmente al Sistema de Información.

De acuerdo con la respuesta realizada por el Grupo de Tecnologías de la Información de la DVR mediante Rad. 20144400146223 se informa:

> Se hará la revisión del documento del Plan de Contingencia de manera integral para actualizar aquella información que no corresponde actualmente al Sistema de Información.

Consideraciones de la Oficina de Control Interno: Teniendo en cuenta que se realizará la revisión del plan de contingencia de manera integral, se recomienda documentar las acciones que sean orientadas al control y actualización de los documentos del Sistema de Información.

Oportunidad de Mejora No. 5

Durante la revisión del documento Plan de Contingencia de los aplicativos de la Dirección de Vigilancia de las Regalías se observó para el Sistema Gesproy SGR, que si bien el plan de contingencia atiende todo lo relacionado a la capa de persistencia (base de datos) y a las capa de negocio y presentación, no se cuenta con evidencia que soporte que se ha probado lo referente a la contingencia de las capas de negocio y de presentación.

Por lo anterior y en consideración a que el Plan de Contingencia está definido en el mapa de riesgos del Sistema de Información como un Control y dada su aplicación parcial, se genera el riesgo de incumplimiento de la actividad No.2 “Aplicar Controles” del Proceso de Seguridad de la Información del Sistema de Gestión de Calidad del DNP, que establece: “Aplica los controles para administrar los riesgos en seguridad de la información”. La no aplicación integral del control definido para éste Sistema de Información, lo deja expuesto a la materialización de los riesgos “Daño de la Información en SGR”, “No disponibilidad de la información en SGR”, definidos en el mapa de riesgos del mismo Sistema.

Recomendación

Se recomienda realizar y documentar las pruebas del plan de contingencia de forma completa que incluya toda la solución, es decir, la capa de persistencia, la capa de negocio y la capa de presentación.

De acuerdo con la respuesta realizada por el Grupo de Tecnologías de la Información de la DVR mediante Rad. 20144400146223 se informa:

> Se realizará y documentará las pruebas del plan de contingencia de forma completa que incluya toda la solución, es decir, la capa de persistencia, la capa de negocio y la capa de presentación.

Consideraciones de la Oficina de Control Interno: Teniendo en cuenta que se realizará la revisión del plan de contingencia de manera integral, se recomienda documentar las acciones que sean orientadas a la realización de pruebas sobre las capas del Sistema de Información.

9. CONCLUSIONES

De acuerdo con las actividades previstas en el plan operativo del año 2014, la Oficina de Control Interno evaluó en forma independiente, con sujeción a las normas generales de auditoría integral, el sistema de control interno inherente al Sistema de Información GESPROY SGR en lo relacionado con la aplicación de las políticas de seguridad de activos de información y Recursos Humanos.

Los resultados de las pruebas practicadas y la evidencia obtenida de acuerdo con los criterios definidos en la planeación del trabajo se refieren sólo a los registros y/o documentos examinados, no se hacen extensibles como conclusión general del estado del Sistema de Información, teniendo en cuenta que la evaluación es selectiva y las muestras fueron tomadas aleatoriamente.

El análisis de los resultados de esta evaluación permite concluir que el sistema de control interno vinculado con el Sistema de Información GESPROY SGR está comprometido con el proceso de mejora continua y puede establecer, a partir de las Oportunidades de Mejora identificadas, mecanismos o acciones que fortalecen este proceso para cada uno de los aspectos evaluados, teniendo en cuenta para ello las recomendaciones que se presentan al Sistema de Información.

Con el propósito de contribuir al fortalecimiento del Sistema de Control Interno Institucional, se requerirá de la formulación de acciones preventivas para las oportunidades de mejora identificadas en el presente informe y relacionadas en la matriz de oportunidades de mejora.

El conjunto de acciones generadas serán objeto de seguimiento por parte de la OCI.