

 **Bogotá, 31 de julio de 2017**

**Distribuido a:**

**Roger Quirama García**

Jefe Oficina de Tecnologías de la Información y las Comunicaciones

**Jaime Humberto Jimenez Vergel**

Coordinador Grupo de Servicio al Ciudadano Institucional

**Francisco Camargo Salas**

Director Dirección Empleo Público

**Guillermo Martinez Daza**

Jefe Oficina Asesora de Planeación

**Alejandro Becker Rojas**

Director Desarrollo Organizacional

 **Copias**

**Liliana Caballero Duran**

Directora

**Emitido por:**

**Luz Stella Patiño Jurado**

Jefe Oficina Control Interno

**Emitido por:**

 Informe de auditoría

Sistema de Información SIGEP

Resumen ejecutivo auditoría al Sistema de Información y Gestión del Empleo Público “SIGEP”

**Objetivo:**

Evaluar la efectividad de la gestión de riesgos y control tecnológico inmerso en la operación del Sistema de Información y Gestión del Empleo Público SIGEP, el cual hace parte de la oferta de sistemas de información que el Gobierno Nacional desarrolla y que constituye una herramienta de gestión de la información de las instituciones y del personal al servicio del estado. Esta evaluación tiene el propósito de retroalimentar al Departamento Administrativo de la Función Pública con oportunidades de mejora que contribuyan al cumplimiento de los objetivos estratégicos definidos por la Entidad.

*Es importante mencionar que las observaciones registradas en el presente informe coadyuvan no solo a fortalecer el ambiente de control y seguridad del sistema de información actual, sino que propositivamente refuerzan la ejecución a futuro de varias actividades de control inmersas en el modelo técnico y operativo plasmado en los estudios previos del SIGEP II, el cual se espera que a mediano plazo presente mayores facilidades para su actualización, mejores servicios transaccionales para los usuarios y mayor eficiencia acorde con las nuevas tendencias tecnológicas que el mercado ofrece y que el Estado necesita.*

**Alcance:**

El Sistema de información SIGEP, de acuerdo con su objeto debe concentrar un gran volumen de información de alta importancia, relacionada con hojas de vida, bienes y rentas, estructuras de planta y contratos de prestación de servicios, entre otros (Ver cuadro siguiente); lo que exige el establecimiento de un entorno tecnológico y de seguridad de la información sólido y determinado bajo las mejores prácticas reconocidas a nivel mundial. Esto hace que los riesgos reputacionales, legales y financieros que se pudieran materializar a causa de la pérdida de la integridad, confidencialidad y disponibilidad de la información por diversos factores sean minimizados.



**Fuente: Reporte volumen de información manejado por SIGEP (Dirección de Empleo Público, corte enero 2017).**

Por las razones antes expuestas, la auditoría determinó efectuar una evaluación a los ambientes de Pre Producción (Red Función pública a nivel de capas de negocio y presentación) y Producción (Red Nube Pública a nivel de capas de negocio y presentación / Red Nube privada capa de negocio y Supervisión Contractual). Siendo áreas objeto de estudio: La Oficina de Tecnologías de la Información y las Comunicaciones “OTIC”, la Dirección de Empleo Público “DEP”, la Oficina Asesora de Planeación “OAP” y el Grupo de Servicio al Ciudadano Institucional “GSCI”.

Con relación a lo anterior, se evaluaron los controles de Tecnología de la Información enfocados en los siguientes dominios:

* Seguridad:
* Gestión de acceso (Validación de usuarios y perfiles) y segregación de funciones
* Aseguramiento S.O. y B.D. (Verificación líneas base de seguridad - Hardening)
* Controles de balanceo de integridad de la información entre componentes (Interfaces).
* Generación y gestión de pistas de auditoria (Logs).
* Operaciones:
* Gestión de incidentes
* Procedimientos de contingencia
* Planes de continuidad.
* Gestión de copias de respaldo y recuperación
* Supervisión contractual servicio de Housing (Administración externa de infraestructura propietaria) nube privada.
* Desarrollo:
* Administración de cambios

**Limitación en el alcance:**

No se presentaron limitaciones en el alcance planeado.

**Interpretación de los resultados de la auditoría:**

Los aspectos evaluados en el proceso de auditoria tienen la siguiente interpretación según sus resultados; la cual indica el grado de cumplimiento de los controles establecidos en el proceso o el impacto que supone la carencia o debilidad de estos, algunas de las observaciones son de responsabilidad directa de la OTIC y otras deben ser solucionadas con el apoyo de diferentes áreas objeto de la auditoría.



Riesgos evaluados

| **Riesgos Identificados en el proceso de auditoría** | **Cubierto en el alcance de la auditoría** | **Calificación de riesgo inherente** **según matriz de riesgos del proceso** |
| --- | --- | --- |
|  |  |
| Accesos no autorizados, causados por: falencias en los controles de seguridad, suministro de claves personales a personas no autorizadas, falencias en la actualización de personal y accesos inactivos.  | Si | Moderado |
| Afectación de la infraestructura tecnológica a causa de: Manipulación inadecuada en la infraestructura tecnológica, fallas u obsolescencia de elementos que componen la infraestructura tecnológica, fallas en niveles de mantenimiento y soporte.  | Si | Alto |
| Inadecuados servicios de Tecnologías de la Información debido a: incorrecta definición o carencia de Acuerdos de Niveles de Servicio, capacidad operativa insuficiente, falta de conocimientos del personal, Inadecuada clasificación de los incidentes reportados por parte de los usuarios. | Si | Alto |
| Pérdida de información o integridad de la misma como consecuencia de: falencias en la generación de copias de seguridad de los equipos servidores, fallas en la infraestructura tecnológica, Falencias en los controles de seguridad informática. Incluido en la matriz de riesgos del proceso “Tecnologías de la Información”. | Si | Extremo |
| Pérdida de trazabilidad de la información debido a la ausencia o deficiencia en los registros, pistas o Logs de auditoria que permitan una investigación forense en las plataformas. Genera | Si | No está identificado y evaluado en la matriz de gestión de riesgos. |

Resultados aspectos evaluados

|  |  |  |
| --- | --- | --- |
| **Detalle de las validaciones realizadas** | **Resultado** | **Oportunidad de mejora** |
| Dominio Seguridad - Aseguramiento S.O. y B.D: Aplicación de parches de seguridad actualizados, asignación de usuarios de operación, parametrización para recuperación de la información completa de la base de datos ante una falla del sistema, controles de acceso remoto y controles sobre modificación directa de datos en la B.D. |  |  |
| Dominio Seguridad-Gestión de acceso: gestión de usuarios para el sistema de información SIGEP |  | **Observación GH01** |
| Dominio Seguridad-Gestión de acceso: Asignación de nombres de usuarios administradores en Sistemas Operativos y Bases de Datos usados para la operación del Sistema de Información. |  | **Observación GH02** |
| Dominio Seguridad - Aseguramiento S.O. y B.D: Líneas base de seguridad. |  | **Observación GH03** |
| Dominio Seguridad - Aseguramiento S.O. y B.D: Parámetros de seguridad B.D. |  | **Observación****GH04** |
| Dominio Seguridad - Aseguramiento S.O. y B.D: Log de Auditoria |  | **Observación****GH05** |
| Dominio Seguridad Generación y gestión de pistas de auditoria LOGs |  | **Observación****GH06** |
| Dominio Operaciones – Gestión de incidentes |  | **Observación GH07** |
| Dominio Operaciones – Plan de continuidad |  | **Observación GH08** |
| Dominio Operaciones – Supervisión Contractual Nube Privada |  | **Observación GH09** |
| Dominio Operaciones – Gestión de copias de respaldo y recuperación |  | **Observación** **GH10** |
| Dominio Desarrollo – Administración de cambios |  | **Observación GH11** |

Observaciones

* **GH01 – Usuarios internos (DAFP código 022) retirados y no identificados que se mantienen aún activos en el sistema de información SIGEP:**

De un universo total de setecientos diez y ocho (718) funcionarios internos del DAFP, registrados en el Sistema de Información con estado activo (Fecha de corte 23 de junio de 2017), se evidenció en el análisis efectuado que cuatrocientos trece (413) corresponden a usuarios que ya no debiesen estar activos por cuestiones de retiro (Planta Global/Temporal), terminación de contrato (Contratistas) o porque son usuarios no identificados. A continuación, se relaciona la cantidad de usuarios por tipo de inconsistencia:

* Ciento cincuenta y dos (152) contratistas cuyos contratos están vencidos desde el año 2012 al 2016 (151 con rol EMPLEADO y 1 con rol EMPLEADO y ROL\_DAFP\_DDO).
* Doscientos trece (213) usuarios no identificados. Se aclara que no aparecen en las bases de información entregadas por el Grupo de Gestión Humana (Planta global, temporales, contratistas y retirados del año 2015 y 2016); de estos, se evidencian 205 usuarios con rol EMPLEADO y 8 con los siguientes roles:

|  |  |  |  |
| --- | --- | --- | --- |
| **USUARIO** | **IDENTIFICACION** | **COD. PERSONA** | **ROL** |
| DALINA PAZ ZAPATA | 34602225 | M2287885 | ROL\_JEFE\_RH\_ENT |
| ROL\_JEFE\_CONTRATOS |
| DANIEL SANCHEZ RIVERA | 1053340444 | M1467482 | ROL\_JEFE\_RH |
| ROL\_JEFE\_CONTRATOS |
| NELCY CARDENAS MORA | 39688322 | M1626419 | ROL\_JEFE\_RH |
| LINA CRUZ SILVA | 52423537 | M551707 | ROL\_ENT\_CI |
| MAURICIO VELOSA CORTES | 80257445 | M123147 | ROL\_JEFE\_CONTRATOS |
| CARLOS MOSQUERA CRUZ | 1020715493 | M375099 | ROL\_GEN\_ENC |
| JANETH CANO | 1121839728 | M1468022 | ROL\_JEFE\_CONTRATOS |
| NUBIA PARRADO GIRALDO | 1121863934 | M1468045 | ROL\_JEFE\_RH |

**Fuente: resultado cruce de información efectuado por la auditoría (base de información de SIGEP Vs la suministrada por él Grupo de Gestión Humana)**

.

* 48 usuarios retirados, aún activos en el sistema de información; todos con el rol EMPLEADO. Seis (6) retirados en 2017, veinticuatro (24) retirados en 2016 y dieciocho (18) retirados en 2015.

Nota: el detalle de las inconsistencias relacionadas se describe en el anexo 1 del presente informe, hoja 1 columna k “validación”.

**Riesgo Evaluado Asociado a la Observación:**

Pérdida de integridad de la información propia del sistema de información, debido a posibles accesos a los datos de SIGEP por personal con rol no autorizado.

**Recomendación:**

* 1. Previa verificación por parte del área responsable, se debe proceder a inactivar los usuarios inconsistentes mencionados en el hallazgo (Ver detalle en el anexo 1). En especial los 8 usuarios no identificados que tienen los roles de Jefe\_RH y Jefe\_Contratos, los cuales “tienen todos los privilegios de consulta, inserción, modificación o borrado de información del servidor público”(Véase PROTOCOLO DE SEGURIDAD, ADMINISTRACIÓN DE USUARIOS Y ROLES SIGEP)

Al depurar los datos de usuarios activos registrados en el SIGEP, por código de entidad y rol asignado se mejora la calidad de datos a migrar a futuro para el nuevo sistema.

* 1. Mantener un estricto control en el procedimiento de inactivación (Retiro) de funcionarios en el sistema de información SIGEP. Es importante implementar en el protocolo de seguridad y administración de usuarios y roles de SIGEP (2015-08-06\_Protocolo\_adm\_usuarios\_roles\_sigep\_v1.pdf) un capitulo donde se determine específicamente el procedimiento de retiro o inactivación de usuarios con los responsables y acciones a ser ejecutadas, además de un procedimiento de monitoreo periódico de usuarios registrados en el sistema.

**Plan de Acción definido por el responsable / Responsable / Fecha de Cumplimiento:**

**N/A –** El Plan de Acción se emite posterior al informe.

* **GH02 – Uso de nombres de cuenta genéricos para la asignación de usuarios administradores:**

Verificando la configuración de usuarios internos para Base de Datos “B.D.” y Sistema Operativo “S.O.”, se evidenciaron aspectos susceptibles a mejorar relacionados con la asignación de nombres genéricos para usuarios de administración, como ejemplo se tienen asignados los siguientes identificadores: “dafpadmin” para S.O. y “sysdba” para B.D, los cuales para el caso del S.O. son manejados por más de un usuario, según se requiera.

**Riesgo(s) Evaluado Asociado a la Observación:**

* Pérdida de integridad de la información, debido a que las cuentas genéricas en usuarios administradores o de altos privilegios son conocidas por contraseñas débiles y muchos accesos pueden ser efectuados desde múltiples equipos, derivando en mayor riesgo de ataques cibernéticos.
* Alto índice de complejidad en el análisis a la trazabilidad de la información, al no poder identificar específicamente que usuario realmente utilizaba la cuenta objeto de investigación.

**Recomendación:**

2.1. Analizar la posibilidad de que los administradores solo usen la cuenta de administración o de altos privilegios a través de una cuenta con identificador personal, con el fin que este identificador no indique sus privilegios.

Este control se debe incluir como normativa en un capítulo dentro de la(s) Guía(s) de administración de cuentas de usuario o de administración, y establecer su parametrización en las líneas base de seguridad de cada plataforma, tal y como se especifica en la siguiente observación.

**Plan de Acción definido por el responsable / Responsable / Fecha de Cumplimiento:**

**N/A –** El Plan de Acción se emite posterior al informe.

* **GH03 – Ausencia de líneas base de seguridad para bases de datos Oracle y Sistemas Operativos Linux y Windows 2012:**

No se evidencian líneas base de seguridad (Hardening) para Sistemas Operativos y bases de datos, específicamente para bases de datos Oracle y para Sistemas Operativos Linux y Windows 2012, que son objeto de análisis por cuanto conforman el soporte del Sistema de Información SIGEP.

Durante la evaluación se encontraron por ejemplo aspectos relacionados con parámetros de contraseña para perfiles en la B.D. Oracle, donde se evidenciaron dos (2) tipos de perfiles “DEFAULT” y “MONITORING\_PROFILE", con parámetros de contraseña diferentes (Parámetros: CONNECT\_TIME, IDLE\_TIME, SESSIONS\_PER\_USER, FAILED\_LOGIN\_ATTEMPTS, PASSWORD \_GRACE\_TIME, PASSWORD\_LIFE\_TIME, PASSWORD\_LOCK\_TIME, PASSWORD\_REUSE\_MAX, PASSWORD\_REUSE\_TIME, PASSWORD\_VERIFY\_FUNCTION). Sobre este aspecto se resalta que no es que la diferencia entre los valores de los parámetros sea problema de seguridad, lo importante es que esta configuración sea soportada por una línea base de seguridad.

A pesar que los parámetros de configuración de seguridad de la B.D. están bajo las mejores prácticas recomendadas ( Accesos de rol público, propietarios de tablas de usuario final, accesos remotos sin autenticación, segregación de usuario con altos privilegios, entre otros) y los de S.O. Linux (Shell restrictivas a líneas de comando, restricciones a servicio FTP activo, método SUDO para acceder con privilegios, entre otros), no se evidencian líneas base de seguridad que soporten esta configuración y que aseguren su grado de actualización en los sistemas y su monitoreo periódico.

**Riesgo(s) Evaluado Asociado a la Observación:**

Pérdida de confidencialidad, integridad y disponibilidad de la información, debido al incremento de incidentes de seguridad, desmejoras en el rendimiento al aumentar los niveles de carga inútil en el sistema, a una administración más compleja y bajos niveles de eficacia en la identificación de problemas.

**Recomendación:**

* 1. Fortalecer el dominio de gestión de la configuración de seguridad en los sistemas del DAFP, mediante la implementación de líneas base de seguridad que permitan preparar los sistemas informáticos y las aplicaciones para resistir de forma adecuada ciberataques conocidos y desconocidos que aprovechan vulnerabilidades para ser cometidos. Específicamente para los elementos que componen la solución SIGEP (S.O., B.D., Servidores, entre otros).

Las líneas base de seguridad deben contener como mínimo:

* Procedimientos de actualización de versiones para S.O. y B.D.
* Configuraciones de seguridad necesarias para protegerse de posibles ataques cibernéticos, como aquellas relacionadas con rutas de acceso compartido, apagado de sistema, inicio y cierre de sesión y opciones de seguridad de red.
* Instalación, configuración y mantenimiento de programas de seguridad tales como: Antivirus, Antispyware y un filtro Antispam según las necesidades del sistema.
* Configuraciones de seguridad orientadas a gestión de usuarios, de políticas de contraseña robusta (Claves caducables, almacenamiento histórico de contraseñas, bloqueos de cuentas por intentos erróneos y requisitos de complejidad de contraseña), renombramiento y posterior deshabilitación de cuentas estándar del sistema, como administrador e invitado (Ver observación GH02), asignación correcta de derechos de usuario, de tal manera que se reduzcan las posibilidades de elevación de privilegios, y tratando siempre de limitar al mínimo los privilegios y/o derechos de los usuarios activos.
* Restricciones de software, basado en lo posible en el uso de listas blancas de software permitido más que en listas negras del mismo (Licenciamiento).
* Activación de auditorías del sistema. Teniendo en cuenta el rendimiento de las máquinas y el consumo de recursos.
* Configuración de servicios de sistema. En este punto es necesario tratar siempre de deshabilitar todos aquellos servicios que no vayan a prestar una funcionalidad necesaria para el funcionamiento del sistema.
* Configuración de acceso remoto. Restricciones de acceso a un número muy limitado de usuarios y al mínimo las conexiones concurrentes, teniendo cuidado en la desconexión y cierre de sesión y el establecimiento de un canal cifrado de comunicaciones para tales propósitos, como SSH, por ejemplo.
* Configuración adecuada de cuentas de usuario, tratando de trabajar la mayor parte del tiempo con cuentas de acceso limitado y deshabilitando las cuentas de administrador. Es absolutamente recomendable usar la impersonificación de usuarios para realizar labores administrativas en vez de iniciar sesión como administradores.
	1. Una vez implementadas en el entorno informático, es fundamental que la entidad establezca procedimientos de control que permitan medir si estas líneas base de seguridad siguen cumpliendo con su objetivo primordial, ejecutando estudios de análisis de vulnerabilidades, los cuales alimentan tanto el proceso de remediación como el proceso de fortalecimiento y la actualización de dichas líneas.

**Plan de Acción definido por el responsable / Responsable / Fecha de Cumplimiento:**

**N/A –** El Plan de Acción se emite posterior al informe.

* **GH04 – Servidores inexistentes o desconocidos con relaciones de confianza a la B.D. de producción de SIGEP:**

Verificando los parámetros de seguridad de la base de datos de producción del sistema de información SIGEP (Tabla SYS.DBA\_DB\_LINKS), se evidenciaron los siguientes servidores los cuales según información del administrador ya no existen, y otros deben ser identificados por el grupo de servicios de información de la OTIC.

* PRUEBAS\_ETB (Ya no existe)
* SIGEPPRU\_ETB (Ya no existe)
* SIGEPPRU\_LINK (Identificar si se debe mantener esta relación)
* DBLINKTEMP LINK (Identificar si se debe mantener esta relación)
* PRUEBA2 LINK (Identificar si se debe mantener esta relación)
* PRUEBA LINK (Identificar si se debe mantener esta relación)

**Riesgo(s) Evaluado Asociado a la Observación:**

Pérdida de integridad y confidencialidad de la información, debido al acceso a los datos mediante un usuario no autorizado que se encuentre matriculado en un servidor con el cual se tengan establecidas relaciones de confianza.

**Recomendación:**

4.1. Eliminar en la tabla SYS.DBA\_DB\_LINKS de la B.D. de producción de SIGEP (Servidores ODA0 y ODA1), los servidores inexistentes o sobre los cuales ya no se deben mantener relaciones de confianza.

4.2. Se debe establecer un control periódico de revisión sobre la debida existencia de estas relaciones en la tabla.

**Plan de Acción definido por el responsable / Responsable / Fecha de Cumplimiento:**

**N/A –** El Plan de Acción se emite posterior al informe.

* **GH05 – Acciones de gestión sobre tablas no incluidas en las opciones de registro del Log de auditoria:**

Revisando las sentencias SQL de la tabla DBA\_STMT\_AUDIT\_OPTS, se encontró que las sentencias INSERT TABLE, DELETE TABLE, UPDATE TABLE, no están siendo auditadas.

**Riesgo(s) Evaluado Asociado a la Observación:**

Pérdida de trazabilidad de la información, debido a la modificación directa sobre los datos de una tabla por usuarios no autorizados, sin poder tener rastro de la información afectada.

**Recomendación:**

5.1. Insertar en la tabla DBA\_STMT\_AUDIT\_OPTS de la B.D. de producción de SIGEP (Servidores ODA0 y ODA1), las opciones de sentencias auditables INSERT TABLE, DELETE TABLE y UPDATE TABLE.

5.2. Se debe implementar un control periódico de revisión sobre la debida configuración de las opciones en la tabla. Este control puede ir ligado a los procedimientos de revisión periódicos sobre las líneas base de seguridad.

Nota: Es importante tener en cuenta esta recomendación para la configuración de seguridad en la trazabilidad de la información del nuevo Sistema (SIGEP 2).

**Plan de Acción definido por el responsable / Responsable / Fecha de Cumplimiento:**

**N/A –** El Plan de Acción se emite posterior al informe.

* **GH06 – Procedimientos de monitoreo y gestión de Logs no evidenciados:**

No se evidencian procedimientos implementados para el monitoreo periódico y gestión de Logs a nivel de la B.D. Oracle 11g, plataforma People net y S.O. Windows 2012 y Red Hat 6.2 que conforman la infraestructura del sistema de información SIGEP.

**Riesgo(s) Evaluado Asociado a la Observación:**

Perdida de integridad de la información, debido a la falta de oportunidad en la detección oportuna de modificaciones o alteraciones no autorizadas sobre los datos o parámetros de configuración del sistema.

**Recomendación:**

6.1. En la actualidad los Logs poseen una gran cantidad de funcionalidades que aportan gran valor para los sistemas, como procesos de optimización, registro de acciones de usuarios para auditorias o fuente de información para investigación de actividades maliciosas (Auditorias forenses). Por tal razón, se hace necesario el establecimiento de una política de gestión de Logs y un procedimiento de control de monitoreo periódico sobre los Logs de operación y auditoria del sistema (S.O. y B.D.), y de las aplicaciones críticas del negocio.

Según las normas NIST SP 800, “Todas las organizaciones deben desarrollar un proceso estándar para la implementación del manejo de los Logs. Como parte del proceso de planeación, la organización debe definir cuáles son sus necesidades y objetivos de la generación de Logs. En base a estas, se deben definir políticas con los requerimientos indispensables y algunas recomendaciones para cada una de las etapas de los procesos de administración de Logs (Generación, transmisión, almacenamiento, análisis y liberación). Los requerimientos y recomendaciones deben generarse teniendo en cuenta un análisis detallado de las tecnologías disponibles, sus implicaciones de seguridad, el costo de implementación y las leyes por las cuales se rige la organización”.

**Plan de Acción definido por el responsable / Responsable / Fecha de Cumplimiento:**

**N/A –** El Plan de Acción se emite posterior al informe.

* **GH07 – Ausencia de indicadores de gestión de incidentes y de Acuerdos de Nivel Operacional “OLA” entre áreas responsables:**

A la fecha de evaluación no se tiene un esquema de indicadores establecido para la medición de la gestión de incidentes en el sistema de información SIGEP, en el cual participen transversalmente todas las áreas intervinientes (GSCI, DEP, DDO y OTIC).

Otro aspecto importante evidenciado por la auditoria, es la inexistencia de OLA internos entre las áreas de soporte. Si bien, se tienen unos ANS (Acuerdos de Nivel de Servicio) generales para la atención de peticiones, quejas, reclamos, sugerencias y denuncias, publicado en la página WEB de la Función Pública (http://www.funcionpublica.gov.co/protocolos-y-niveles-de-servicio), estos no tienen en cuenta la integración de los tiempos que realmente dura el escalamiento al interior de cada una de las áreas de soporte.

**Riesgo(s) Evaluado Asociado a la Observación:**

Posible pérdida de disponibilidad e integridad de la información, debido a un deficiente tratamiento de incidencias técnico-operativas en el sistema, al presentarse los siguientes factores de riesgo:

* Inexistente o inadecuado establecimiento de indicadores que permitan medir la efectividad en la gestión.
* Incumplimiento de los ANS u OLA, debido a un dimensionamiento deficiente en la información de tiempo de resolución independiente por cada área responsable.

**Recomendaciones:**

* 1. Implementar un esquema de indicadores de gestión de incidentes, el cual permita mediante sus servicios de reporte y consulta, la medición periódica de la efectividad de dicha gestión. Es importante y fundamental que se involucren a todas las áreas responsables para la solución de incidentes a nivel 1y 2, teniendo como objeto mínimo el cumplimiento de los ANS y OLA (General e interno por área responsable), el análisis de incidencias repetitivas, el dimensionamiento y capacidad de los recursos informáticos y la capacitación de los recursos humanos, entre otros.
	2. Establecer OLA internos entre el DEP y la OTIC, que determinen las actividades y los tiempos reales de resolución de incidentes que debe surtir cada uno a través del ciclo de vida de gestión y acorde con su tipología, con el fin de establecer claramente las responsabilidades de cada interviniente, y la integralidad total de tiempos de solución que deben realmente conformar el tiempo total en el ANS Global de la Entidad.

**Plan de Acción definido por el responsable / Responsable / Fecha de Cumplimiento:**

**N/A –** El Plan de Acción se emite posterior al informe.

* **GH08 – Falta de componentes fundamentales en el plan de continuidad del DAFP y de SIGEP acorde con las mejores prácticas**

Basados en las mejores prácticas soportadas por la norma ISO 22301:2012 para la Gestión de la Continuidad del Negocio. Esta auditoría no evidenció los siguientes aspectos que deben hacer parte del plan y que se consideran importantes para la minimización de los riesgos inherentes a la Continuidad del Negocio:

1. Una vez revisado el Plan de Continuidad del Negocio remitido por la Oficina Asesora de Planeación, se relacionan los siguientes elementos, los cuales no han sido implementados:
* Política de continuidad del negocio: donde se establezcan los objetivos, el contexto, el marco de gobierno y el alcance del plan.
* Planes de formación: Donde se especifiquen las necesidades continuas de formación y nivel de competencia del personal cuyos roles soportaran el manejo de la crisis.
1. No se evidencian claramente los análisis de impacto (BIAs) de los procesos y servicios del Departamento.
2. Verificando el plan de continuidad consolidado (2017-04-28\_Plan\_continuidad\_consolidado.xlsx), suministrado por la Oficina Asesora de Planeación, se observa que:
* No hay evidencia de la participación de las áreas misionales, en especial las Direcciones de Empleo Público y Desarrollo Organizacional quienes soportan en mayor grado la operación funcional del sistema de información SIGEP.
* Se presenta incumplimiento en los tiempos programados de finalización (30 de junio 2017) de la actividad “8.4. Analizar los planes de continuidad y recuperación y elaborar el cronograma de pruebas de los planes de continuidad y recuperación de la infraestructura tecnológica”, y “9.2. Analizar los planes de continuidad y recuperación y elaborar el cronograma de pruebas de estos planes de continuidad Arregle y recuperación de los servicios de TI”, asignada a la OTIC como dependencia responsable; esto debido a que a la fecha en el plan de continuidad y recuperación de SIGEP no se ha generado este cronograma.
1. Con respecto al plan de continuidad de SIGEP (2017-05-09\_Plan\_de\_continuidad\_sigep.docx), no se evidencia en el sistema de la Mesa de Servicio (Herramienta Proactiva Net), el “Plan de recuperación de Plataforma Física y de Virtualización”, mencionado en el documento dentro de los planes de recuperación requeridos.

**Riesgo(s) Evaluado Asociado a la Observación:**

Pérdidas de imagen y/o económicas, debido a fallas en la disponibilidad de la información, por la ausencia o inadecuada definición de DRP y BIA corporativo para la infraestructura tecnológica, y/o a la ausencia o inadecuada definición de planes de contingencia sobre plataformas críticas.

**Recomendaciones:**

* 1. Implementar una Política de Continuidad de Negocio para el Departamento; la cual debe determinar para todos los servidores de la Función Pública y demás involucrados el grado de obligatoriedad en la gestión de dicho plan.

Mediante esta Política se debe establecer el marco para el desarrollo, implantación, revisión y mejora de los planes de continuidad del negocio en la Función Pública, con el fin de posibilitar una respuesta adecuada y oportuna ante la materialización de un riesgo de   seguridad de características catastróficas, que provoquen un escenario de falta de disponibilidad de alguno de los componentes básicos de la actividad del Departamento, y que mitigue la repercusión de las posibles catástrofes sobre las actividades del negocio, garantizando que se preservan los datos y funciones esenciales o, de no ser posible, que tales datos o funciones se recuperen, oportuna y progresivamente, hasta la vuelta a la normalidad de la operación.

* 1. Establecer planes de formación, donde se especifiquen las necesidades continuas de formación y nivel de competencia del personal cuyos roles soportarán el manejo de la crisis; estos deben ser revisados y actualizados periódicamente.

* 1. Desarrollar los BIA por proceso, acorde con el trasfondo tecnológico, operativo y estratégico, en ellos se debe tener en cuenta:
* La descripción de las actividades vitales del proceso frente a los servicios ofrecidos a sus steakholders y que se vean afectados en un evento disruptivo. Para ello se debe sopesar si cada actividad es crítica para la continuidad de la Función Pública.
* La determinación de los tiempos en que deben recuperarse los servicios después de una contingencia, para no afectar la continuidad del negocio de la Empresa.
* El personal crítico requerido (Cantidad, rol a desempeñar, datos personales de contacto), los recursos informáticos, equipos y elementos necesarios por cada responsable, los proveedores críticos y los tipos de riesgos que se han identificado en el proceso, que puedan afectar los servicios ofrecidos a sus clientes internos o externos.
	1. Incluir a las áreas misionales en el desarrollo del plan de continuidad. Para el caso del SIGEP específicamente las Direcciones de Desarrollo Organizacional y Empleo Público, para considerar la transversalidad de todos los procesos que soportan tecnológica y operativamente la gestión del sistema, estas últimas consideradas como el front de acceso, gestión o consulta de la información. En el desarrollo de la auditoría se observó por ejemplo con la Dirección de Empleo Público, que no tienen conocimiento sobre el plan de continuidad del negocio, y por ende no se ha desarrollado nada al respecto.
	2. El líder a cargo de coordinar el plan de continuidad consolidado, así como los responsables por proceso, deben establecer un estricto seguimiento al cumplimiento de los tiempos de compromiso en el desarrollo de las actividades establecidas en el plan consolidado, así como a sus posibles desviaciones.
	3. La OTIC debe asegurar la generación de todos los planes de recuperación relacionados en plan de continuidad del SIGEP (2017-05-09\_Plan\_de\_continuidad\_sigep.docx), teniendo en cuenta que durante el proceso de auditoria no se evidenció el “Plan de recuperación de Plataforma Física y de Virtualización” relacionado. Lo anterior para dar cumplimiento al numeral 8.3 “Parametrizar los planes de continuidad y recuperación de la infraestructura tecnológica en la herramienta de mesa de servicio” (Plan de Continuidad Consolidado); se observó que la actividad en mención no fue cumplida en el tiempo establecido en el cronograma (28 de abril del año en curso).

**Plan de Acción definido por el responsable / Responsable / Fecha de Cumplimiento:**

**N/A –** El Plan de Acción se emite posterior al informe.

* **GH09 – Responsabilidades de Gestión de seguridad y Continuidad de operaciones del proveedor del servicio de data center (Housing), no supervisadas por la administración del contrato.**

Verificando la gestión de la supervisión del contrato por parte de la Función Pública, con respecto al cumplimiento de las responsabilidades del proveedor, relacionadas con la gestión de seguridad y las condiciones de servicio de continuidad, las cuales están estipuladas en la ficha técnica (Anexo 6) del “Acuerdo marco de precios CCE-134-1-AMP-2014, celebrado entre Colombia Compra Eficiente y Unión Temporal S&S”, cuyo objeto es el establecimiento de las “Condiciones en las cuales los proveedores deben prestar a las Entidades Compradoras los Servicios de conectividad y Centro de Datos/Nube privada y la forma como las Entidades Compradoras contratan estos servicios”. Teniendo en cuenta el seguimiento de la Oficina de Control Interno a la supervisión de éste contrato por parte del Departamento, se evidenciaron que a las siguientes responsabilidades no se les ha efectuado el seguimiento:

***ANEXO No. 6:***

***“CONDICIONES DE SERVICIO TRANSVERSALES A TODOS LOS NIVELES DE SERVICIO:***

Seguridad:

* Protección antivirus y malware (con actualizaciones de las definiciones dentro de las 24 horas).
* Control de acceso físico al Centro de Datos.
* Protocolos de seguridad utilizados para la administración remota (por ejemplo, SSL, SSH, RDP, etc.).
* Eliminación de todas las contraseñas por defecto y el acceso para invitados.
* Uso obligatorio de los acuerdos de no divulgación (NDA) para el personal proveedor.
* Protocolos para retención y eliminación de datos.

Gestión de seguridad:

* Centro de Operaciones de Seguridad o Security Operations Center (SOC) 7x24 para gestión de seguridad de los servicios ofertados, de tal manera que el proveedor cuente con un centro de monitoreo de los incidentes de seguridad que se puedan presentar y de manera proactiva pueda gestionar los riesgos, asegurando así las condiciones de servicio.
* La gestión incluye la notificación de incidentes de seguridad a las Entidades Compradoras.

***CONDICIONES DE SERVICIO POR NIVEL DE SERVICIO (ORO):***

* Instalaciones de Centro de Datos y sus subsistemas (Tipo Tier 3 o superior o similar).

***CONDICIONES DE SERVICIO DE CONTINUIDAD POR NIVEL DE SERVICIO:***

|  |  |
| --- | --- |
| Falla en Almacenamiento | Replicación (asincrónica/sincrónica) por almacenamiento |
| Falla en Comunicaciones | Enlaces redundantes |
| Capacidad de recuperación | Hasta 6hr para restauración de datos por cada 10TB o menos; y proporcional\*. Proporcional por cada 10TB; ejemplo, hasta 20TB entonces se duplica el tiempo máximo a 12hr.  |
| Contingencia centro alterno | Esquema activo-pasivo, y opcional esquema activo-activo |

 **Fuente; Anexo No. 6 del Acuerdo marco de precios CCE-134-1-AMP-2014”**

***Acuerdo Marco:***

***“Clausula 3.5***

El proveedor debe garantizar el mantenimiento de la infraestructura y de sus componentes para garantizar la prestación del servicio.

***Clausula 11 Obligaciones del proveedor:***

* 11.20. Establecer planes de contingencia cuando ocurran eventos de fuerza mayor o caso fortuito que afecten la prestación de los servicios de conectividad y centro de datos/nube privada.
* 11.23. Contratar a un tercero que realice pruebas de seguridad a la infraestructura utilizada para los servicios de conectividad y centro de datos/nube privada”.

**Riesgo(s) Evaluado Asociado a la Observación:**

Pérdida en la disponibilidad de la información, debido a fallas en la plataforma SIGEP, que ocasionan su indisponibilidad y un incumplimiento de la promesa de servicio.

**Recomendaciones:**

9.1. La supervisión del contrato debe establecer un control de vigilancia periódica y permanente a la correcta ejecución del objeto contratado, tal y como lo especifica la Resolución No. 251 de 2015. Para el caso del contrato en mención, se deben coordinar visitas de seguimiento con el proveedor, donde se puedan corroborar las condiciones de servicio ofrecido expuestas en el Acuerdo Marco y el Anexo Técnico No. 6, verificando temas de configuración, instalación, acuerdos, protocolos, soportes de gestión, informes de pruebas de seguridad a la infraestructura y de pruebas de los planes de continuidad mencionados, entre otros.

Es Importante que, del resultado de cada verificación periódica, se genere un informe por parte de la supervisión y se anexe a la carpeta o repositorio del contrato.

**Plan de Acción definido por el responsable / Responsable / Fecha de Cumplimiento:**

**N/A –** El Plan de Acción se emite posterior al informe.

* **GH10 – Aspectos susceptibles a mejorar en la gestión de copias de respaldo y recuperación**

Se verificó el procedimiento y los soportes técnicos de la gestión a copias de respaldo y recuperación, encontrándose lo siguiente:

* Las guías de respaldo y recuperación que están actualmente en el repositorio oficial de calidad (“2013-07-13\_Guia\_copias\_seguridad\_v3.pdf” y “2015-07-23\_ Guia\_planificacion\_ejecucion\_backups\_v4.pdf”) se encuentran desactualizadas, no obstante, se evidencia un documento de Políticas de respaldo, custodia y recuperación de la Información elaborado por la OTIC (actualizado a mayo de 2017), el cual no se encuentra publicado en el Sistema de Gestión de Calidad pero si está acorde con la gestión actual realizada.
* El gabinete de almacenamiento interno de cintas ubicado en el Data Center del Departamento, presenta deterioro en el cierre de sus puertas, ocasionando posibles afectaciones a la integridad y seguridad de los medios magnéticos que contienen la información del ambiente de producción del SIGEP.
* No se evidencia un plan de pruebas de restauración de las copias de respaldo tomadas periódicamente, ni los informes y soportes de las pruebas que se han efectuado esporádicamente.

**Riesgo(s) Evaluado Asociado a la Observación:**

Pérdida en la disponibilidad de la información, debido a falencias en la generación o recuperación de copias de seguridad de los equipos servidores.

**Recomendaciones:**

* 1. Oficializar el documento de políticas de respaldo, custodia y recuperación de la Información versión 1.2 (2017\_Política\_Backups\_V1.2.pdf), reemplazando las guías actuales o unificándolas a este solo documento.
	2. Mejorar las condiciones de almacenamiento internas de cintas, mediante la adecuación de un gabinete con las debidas medidas de seguridad de acceso.
	3. Implementar un plan de pruebas de restauración permanente y periódico de las cintas de respaldo, que permita medir la eficacia en la restauración de la información ante eventos de fallo que atenten contra la disponibilidad del sistema. Parte del plan está en mantener los soportes e informes correspondientes a cada prueba.

**Plan de Acción definido por el responsable / Responsable / Fecha de Cumplimiento:**

**N/A –** El Plan de Acción se emite posterior al informe.

* **GH11 – Inexistencia de un contrato de soporte de desarrollo del sistema de información SIGEP.**

Evaluando el procedimiento para el control de cambios, se evidenció un control adecuado a nivel de la gestión del procedimiento y de los ANS establecidos hasta donde se tuvo vigente el contrato No. 101 de 2016, con el proveedor de servicio de soporte técnico especializado HEINSOHN, el cual tuvo un plazo de ejecución hasta diciembre de la vigencia pasada. A la fecha de elaboración de éste informe y una vez revisada la carpeta contractual, se evidencia que en noviembre 4 del año pasado solo se realizó una adición al valor del contrato por $ 115.197.0000, pero no obra prórroga al plazo de ejecución del mismo; ocasionando con ello la inexistencia de soporte técnico especializado, para el desarrollo ante fallos o incidentes que llegarán a presentarse en el sistema de información SIGEP.

Actualmente se encuentran dos (2) requerimientos desde enero del presente año pendientes de solución en mesa de servicio (Proactiva Net) por este motivo: REQ 2016-034340 - SCC299\_Formulario de Gerentes públicos- Estado en Pruebas y REQ 2016-030855- Interoperabilidad CNSC Distrital- Alcance- validación.

**Riesgo(s) Evaluado Asociado a la Observación:**

Pérdida de oportunidad en la resolución de nuevos requerimientos en la plataforma que afecten su funcionalidad y por ende la calidad del servicio.

**Recomendaciones:**

11.1. Establecer de manera inmediata un nuevo contrato de soporte especializado para el desarrollo del SIGEP; de no ser así el sistema no estaría habilitado para gestionar el objeto sobre el cual fue diseñado ante cualquier eventualidad (fallo o incidente) que afecte su operación.

**Plan de acción definido por el responsable / Responsable / Fecha de cumplimiento:**

**N/A –** El Plan de Acción se emite posterior al informe.

**Luz Stella Patiño Jurado**

Jefe Oficina Control Interno

Elaboró: Ingeniero Juan Mauricio Cornejo Rodríguez