SUPERINTENDENCIA DE LA ECONOMIA SOLIDARIA

SEGUIMIENTO DIAGNÓSTICO INTEGRAL DE LA PLATAFORMA DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN DELOITTE & TOUCHE (GESTION DE INFRAESTRUCTURA)

OFICINA DE CONTROL INTERNO

Bogotá, D.C, Noviembre de 2016

1. Objetivo

Efectuar seguimiento a la implementación de acciones a las recomendaciones efectuadas por la firma Deloitte & Touche, sobre el diagnóstico integral de la plataforma de tecnología y sistemas de información de la Superintendencia de la Economía Solidaria.

2. Alcance

Se realiza seguimiento a las recomendaciones establecidas en los nueve (9) informes elaborados por la firma Deloitte & Touche (emitidos en noviembre y diciembre del año 2014), relacionados con el diagnóstico integral de la plataforma de tecnología y sistemas de información, con corte al mes de noviembre del año 2016.

3. Desarrollo

Los siguientes son los nueve (9) objetivos establecidos por la firma Deloitte & Touche en auditoria externa, sobre el diagnóstico integral de la plataforma de tecnología y sistemas de información:

Objetivo 1 Diagnóstico de los sistemas de información, plataforma y recursos tecnológicos con los que cuenta actualmente la Superintendencia de la Economía Solidaria	Objetivo 2 Diagnóstico del estado de seguridad de la plataforma tecnológica de la Superintendencia de la Economía Solidaria	Objetivo 3 Evaluación de las funciones críticas de tecnología de información
Objetivo 4 Diagnóstico sobre la administración de las bases de datos de la Superintendencia de la Economía Solidaria	Objetivo 5 Diagnóstico sobre las competencias del personal de planta y de contrato de prestación de servicios de apoyo a la gestión que maneja y ejecuta los recursos informáticos de la Compañía	Objetivo 6 Diagnóstico sobre los planes de contingencia de todos los sistemas de información con que cuenta actualmente la Superintendencia de la Economía Solidaria
Objetivo 7 Diagnóstico sobre el diseño, implementación y efectividad de los controles para la administración de la infraestructura tecnológica de Supersolidaria para los sistemas Fábrica de Reportes, Sigcoop y Orfeo	Objetivo 8 Diagnóstico de seguridad de infraestructura tecnológica mediante pruebas Ethical Hacking	Objetivo 9 Revisión del procedimiento de administración de licenciamiento de software

A continuación se presenta el grado de avance de las oportunidades de mejora identificadas en cada uno de los objetivos señalados en la auditoría realizada por la firma auditora externa:

Objetivo 1:

Diagnóstico de los sistemas de información, plataforma y recursos tecnológicos con los que cuenta actualmente la Superintendencia de la Economía Solidaria

SEGUIMIENTO A LOS PROYECTOS DE LA OFICINA DE SISTEMAS		
ITEM	**HALLAZGO**	**RESPUESTA**
1	No se tiene documentado el seguimiento a los proyectos de inversión que no han sido finalizados.	El seguimiento a los proyectos se encuentra registrado en el SPI (Sistema de Seguimiento Proyectos de Inversión) y está disponible para la consulta de cualquier ciudadano
2	No se cuenta con métricas o indicadores que permitan realizar un seguimiento al beneficio esperado de los proyectos que ya han sido ejecutados por la Oficina de Sistemas.	No se emite respuesta por parte de la Oficina Asesora de Planeación y Sistemas.
ITEM	**RECOMENDACIONES**	
1	Definir e implementar mecanismos de medición que permitan conocer el estado de implementación de los proyectos en curso, teniendo en cuenta los siguientes aspectos:	
1.1	Cumplimiento de la metodología de proyectos definida por la entidad	
1.2	Definición de cronogramas de implementación y porcentaje de cumplimiento de las actividades definidas	
1.3	Cumplimiento del presupuesto dentro de los tiempos definidos	
1.4	Actividades de monitoreo para el cumplimiento de los tiempos establecidos	
1.5	Acciones correctivas para las actividades que no se han cumplido dentro de los tiempos planteados.	
2	Definir e implementar medidas que permitan hacer un seguimiento al beneficio esperado de los proyectos, teniendo en cuenta los siguientes aspectos:	
2.1	Definición de métricas o indicadores que permitan comparar el beneficio obtenido frente al beneficio planteado al inicio del proyecto.	
2.2	Revisar el cumplimiento del presupuesto planteado para el proyecto	

DEFINICIÓN DE RIESGOS INFORMÁTICOS		
ITEM	**HALLAZGO**	**ESTADO O AVANCES**
1	No se han contemplado otros factores de riesgo a los que puede estar expuesta la entidad asociados a los recursos, las operaciones, las aplicaciones y la infraestructura tecnológica	Se evaluara con el funcionario encargado la identificación de riesgos adicionales. (Humanos, ambientales, físicos y tecnológicos)
2	No se tiene un inventario de activos de información que permita identificar la clasificación de la información dentro de la entidad, los riesgos a los que se encuentran expuestos y los controles necesarios para mantener su integridad, disponibilidad y confidencialidad.	La segunda recomendación se acepta

ITEM	RECOMENDACIONES
1	Evaluar la posibilidad de incluir en la matriz de riesgos otros factores a los que puede estar expuesta la Oficina de Sistemas y Supersolidaria como pueden ser los recursos, las operaciones, las aplicaciones y la infraestructura tecnológica.
2	Se deben identificar todos los activos de información importantes para la compañía y elaborar y mantener actualizado un inventario de estos activos, de forma que se realice una protección efectiva de los mismos. Este inventario debe incluir por lo menos la siguiente información: Nombre del activo - Propietario - Clasificación de la información - Ubicación - Medidas de seguridad y protección de la información

OBSOLESCENCIA EN LOS EQUIPOS DE CÓMPUTO		
ITEM	**HALLAZGO**	**ESTADO O AVANCES**
1	Identificamos que el 24,5% de la totalidad de equipos de la entidad cuentan con más de 3 años de vida útil	No se acepta la recomendación porque la estrategia está orientada a las necesidades de cada usuario.
ITEM	**RECOMENDACIONES**	
1	Evaluar la posibilidad de realizar una actualización gradual de los equipos de cómputo y servidores de Supersolidaria.	
2	Establecer un control que permita identificar con tiempo suficiente los equipos que están cerca de cumplir su tiempo de vida útil para poder incluirlos dentro de los proyectos de actualización tecnológica del área.	

SUBUTILIZACIÓN DE LOS RECURSOS INFORMÁTICOS DE LA SUPERSOLIDARIA		
ITEM	**HALLAZGO**	**ESTADO O AVANCES**
1	Evidenciamos que el porcentaje de utilización de los recursos es menor al 20%, lo que indica una subutilización de los recursos adquiridos.	No se acepta porque la infraestructura se adquirió para soportar la operación de 4 a 6 años de la entidad, en especial lo que tiene que ver con las NIIF, los modelos de riesgo, el XBRL y la inteligencia de negocios.
ITEM	**RECOMENDACIONES**	
1	Realizar un análisis de la capacidad y desempeño de la infraestructura tecnológica de la entidad con el fin de evaluar si la capacidad de los recursos adquiridos es necesaria para los requerimientos de la entidad.	
2	Definir un procedimiento que permita proyectar las características de la infraestructura tecnológica de acuerdo a la capacidad y desempeño esperado. Dentro de este procedimiento se deben tener en cuenta los siguientes aspectos: - Definir estándares de medición de capacidad por plataforma - Umbrales - Carga de trabajo actuales y tendencias de carga futura de los recursos de tecnología de información - Actividades para el monitoreo de la capacidad y desempeño - Capacidad de almacenamiento de los sistemas de información - Contingencias necesarias - Cantidad de usuarios actuales frente a la demanda futura - Establecer informes del análisis de capacidad y desempeño	

ENCUESTA PARA MEDIR EL GRADO DE SATISFACCIÓN DE LOS USUARIOS FRENTE A LOS SISTEMAS DE INFORMACIÓN CAPTURADOR (SIGCOOP), FÁBRICA DE REPORTES Y GESTIÓN DOCUMENTAL (ORFEO)		
ITEM	**HALLAZGO**	**ESTADO O AVANCES**
1	La gran mayoría de los usuarios ha tenido problemas de disponibilidad con al menos una de las aplicaciones que utilizan. Revisamos y la mayoría presenta problemas con Orfeo.	Se revisarán las observaciones dentro del contexto de la entidad en el entendido de que la oficina ha establecido los lineamientos requeridos para hacer el levantamiento de las necesidades de los usuarios. Orfeo ya no se encuentra en producción.

ITEM	RECOMENDACIONES
1	Realizar un seguimiento de las causas más comunes que afectan la disponibilidad del servicio e implementar controles que permitan minimizar la afectación de incidentes de disponibilidad.
2	Establecer controles alternos que permitan mantener la disponibilidad de las operaciones cuando se presente un incidente de disponibilidad en las aplicaciones o servicios prestados, que permitan al usuario poder cumplir con los términos establecidos por la ley
3	Incluir al usuario final en las etapas relevantes de las mejoras en las aplicaciones o implementación de proyectos, desde la definición de requerimientos, etapas de pruebas y comité de cambios
4	Realizar encuestas periódicas a los usuarios con el fin de evaluar la percepción del servicio y definir acciones correctivas que permitan mejorar los servicios prestados por la Oficina de Sistemas.

Objetivo 2:

Diagnóstico del estado de seguridad de la plataforma tecnológica de la Superintendencia de la Economía Solidaria.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		
ITEM	**HALLAZGO**	**RESPUESTA**
1	No se cuenta con una política que defina los lineamientos de seguridad de la información establecidos para la Supersolidaria.	Se encuentra publicado en Isolucion con los documentos D-GEIN-008 Buenas Prácticas Uso Plataforma Tecnológica F-GEIN Acuerdo Individual Manejo Información
ITEM	**RECOMENDACIONES**	
1	Definir e implementar una política de seguridad de la información que contenga la siguiente información: - Definición de seguridad de la información, sus objetivos generales y su alcance. - Una declaración de la intención de la gerencia, que apoye las metas y los principios de seguridad de la información en línea con la estrategia y los objetivos de negocio. - Un marco para fijar los objetivos de control y los controles, incluyendo la estructura de evaluación de riesgos y gestión de riesgos. - Una explicación breve de las políticas, principios, estándares y requisitos de cumplimiento de importancia particular para la compañía. - Una definición de las responsabilidades generales y específicas para la gerencia de seguridad de la información, incluyendo reportar incidentes de seguridad de la información. - Referencias a la documentación que puede respaldar la política; como políticas, estándares y procedimientos más detallados de seguridad para sistemas de información específicos o reglas de seguridad que deben acatar los usuarios. Entre estas políticas y estándares se deberían incluir: - Política de control de acceso - Política para el usuario final - Política de uso aceptable - Política de clasificación de datos - Políticas de auditoría	
2	La política debe estar aprobada, publicada y comunicada a todos los empleados de la entidad. También debe ser revisada regularmente o si ocurren cambios significativos para asegurar la continúa idoneidad, eficiencia y efectividad.	

DEFINICIÓN DE POLÍTICAS DE CONTRASEÑAS		
ITEM	**HALLAZGO**	**RESPUESTA**
1	No se cuenta con una política formal de contraseñas para la Supersolidaria	Se acepta y se actualizará el documento de Acuerdo Individual Manejo Información
ITEM	**RECOMENDACIONES**	
	- Definir e implementar una política de contraseñas y acceso lógico que defina los lineamientos generales para establecer la complejidad de las contraseñas en todos los sistemas de información de la Supersolidaria. Este documento debe ser revisado y aprobado por la alta gerencia y asegurar que sea conocida por toda la Supersolidaria. - Adicionalmente asegurar que dentro de la política se incluya la definición de los siguientes aspectos: - Longitud mínima de contraseña - Complejidad de contraseña para todos los sistemas de información. - Histórico de contraseña - Vigencia mínima de la contraseña - Vigencia máxima de la contraseña - Número de intentos fallidos de acceso antes del bloqueo de la cuenta	

PLAN DE TRABAJO CONTROLADOR DE DOMINIO		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Identificamos que dos usuarios que hacen parte de grupos administradores no están siendo utilizados	Los usuarios ya están bloqueados
ITEM	**RECOMENDACIONES**	
1	Evaluar la posibilidad de bloquear o eliminar los usuarios que hacen parte de los grupos administradores del controlador de dominio y que no están siendo utilizados actualmente.	

USUARIO CON ACCESO NO AUTORIZADO A LAS UNIDADES DE DISCO O RUTAS COMPARTIDAS		
ITEM	**HALLAZGO**	**RESPUESTA**
1	identificamos que el usuario S-1-5-21-1993962763-1647877149-1801674531-4729 tiene permisos no autorizados a unidades y carpetas compartidas del controlador de dominio	El usuario ya fue eliminado
ITEM	**RECOMENDACIONES**	
1	Evaluar la posibilidad de restringir los permisos de acceso del usuario S-1-5-21-1993962763-1647877149-1801674531-4729 a las unidades de disco y rutas compartidas del controlador de dominio.	

DEFINICIÓN DE COMPLEJIDAD DE CONTRASEÑAS		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Identificamos parámetros que no están alineados con las buenas prácticas de seguridad.	Aceptamos revisar la implementación de estos parámetros de acuerdo a la situación actual de la entidad.
ITEM	**RECOMENDACIONES**	
1	Evaluar la viabilidad técnica de alinear los parámetros de contraseña acorde a las buenas prácticas que se mencionan a continuación:	

Parámetro	Valor recomendado por las buenas prácticas
Permitir bloqueo de cuenta administrador	Enabled
ForceLogoffWhenHourExpire	TRUE(Enabled)
LockoutBadCount	3 attempts
LockoutDuration	Greater than 0 minutes
MinimumPasswordLength	6 or more characters
PasswordComplexity	TRUE(Enabled)
MaximumPasswordAge	30 to 90 days
PasswordHistorySize	6 or more passwords
Prevent Transfer of Passwords in Clear Text	Enabled
RequireLogonToChangePassword	Enabled
ResetLockoutCount	1440 minutes

ADMINISTRACIÓN DE USUARIOS		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Identificamos dos usuarios habilitados y que no tienen fecha de ingreso al sistema.	Se acepta. Se depurara los usuarios reportados en la observación.
ITEM	**RECOMENDACIONES**	
1	Evaluar la posibilidad de implementar las siguientes recomendaciones de acuerdo con las buenas prácticas: - Bloquear o eliminar los usuarios que nunca han accedido al sistema. - Activar la expiración de la contraseña para los usuarios identificados. - Renombrar la cuenta administrador dentro de controlador de dominio. En caso de que no se vayan a modificar las cuentas de usuario reportadas, incluir estas cuentas en un documento formal, revisado y aprobado por la Oficina de Sistemas de Supersolidaria con el respectivo análisis de riesgos asociado a dicha definición.	

SERVICIOS DE RED		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Realizar un análisis sobre los servicios mencionados en la observación para evaluar la necesidad de tenerlos activos o deshabilitarlos en el sistema operativo, considerando los riesgos que esto puede representar.	Se quita la observación
ITEM	**RECOMENDACIONES**	
1	Realizar un análisis sobre los servicios mencionados en la observación para evaluar la necesidad de tenerlos activos o deshabilitarlos en el sistema operativo, considerando los riesgos que esto puede representar.	

POLÍTICAS DE AUDITORÍA EN EL CONTROLADOR DE DOMINIO		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Identificamos que las siguientes políticas de auditoría no están activas en el directorio activo	Se acepta. El controlador de dominio fue instalado recientemente y esta implementación hace parte de la siguiente etapa.

ITEM	RECOMENDACIONES
1	Evaluar la viabilidad técnica de habilitar acorde a las buenas prácticas las políticas de auditoría en el controlador de dominio. Adicionalmente se deben realizar revisiones periódicas sobre los registros almacenados de forma que se puedan identificar incidencias de seguridad.

PLAN DE TRABAJO SERVIDOR ORFEO		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Identificamos que los siguientes grupos no tienen usuarios asignados: tty, disk, kmem, dialout, fax, voice, floppy, tape, audio, operator, src, shadow, utmp, video, sasl, staff, users, crontab, fuse, mlocate, ssh, winbindd_priv, netdev, rvm.	Se revisaran las observaciones y se aplicaran las que se consideren válidas, toda vez que el aplicativo ya no se encuentra en funcionamiento, solo está disponible para consulta.
ITEM	**RECOMENDACIONES**	
1	Realizar un análisis sobre los grupos que no tienen asociados cuentas de usuario, para determinar la necesidad de mantenerlos o eliminarlos del sistema.	

PARÁMETROS DE CONTRASEÑAS EN EL SERVIDOR ORFEO		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Durante la ejecución del plan de trabajo de Ubuntu en el servidor de Orfeo, revisamos los parámetros de contraseña en el servidor e identificamos lo siguiente: Parámetros Valor configurado Políticas de Supersolidaria LOGIN_RETRIES 5 intentos No definido LOGIN_TIMEOUT 60 segundos No definido PASS_MAX_DAYS 9999 días 35 días PASS_MIN_DAYS 0 días No definido PASS_MIN_LEN Este parámetro no se encuentra definido. No definido	Se revisaran las observaciones y se aplicaran las que se consideren válidas, toda vez que el aplicativo ya no se encuentra en funcionamiento, solo está disponible para consulta.
ITEM	**RECOMENDACIONES**	
1	Evaluar la posibilidad de técnica de configurar los siguientes parámetros de contraseñas del servidor Orfeo acorde con las buenas prácticas: - LOGIN_RETRIES: 3 intentos - PASS_MAX_DAYS: 30 a 90 días - PASS_MIN_DAYS: 1 día - PASS_MIN_LEN: 8 caracteres	

DEBILIDADES EN LA RESTRICCIÓN DE ACCESOS A LOS NUEVOS ARCHIVOS EN EL SERVIDOR ORFEO		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Evidenciamos que la variable “UMASK” se encuentra configurada en 22, lo cual no se encuentra de acuerdo a las mejores prácticas.	Se revisaran las observaciones y se aplicaran las que se consideren válidas, toda vez que el aplicativo ya no se encuentra en funcionamiento, solo está disponible para consulta.
ITEM	**RECOMENDACIONES**	
1	Evaluar la posibilidad de técnica de configurar los accesos a los nuevos archivos acorde a las buenas prácticas. Tener en cuenta que las mejores prácticas recomiendan un valor de 027 (el dueño del archivo tiene todos los derechos, el grupo no tiene permisos de escritura y los usuarios carecen de permisos sobre el archivo), de manera que sólo el propietario de los archivos tenga permisos de escritura.	

DEBILIDADES EN LA RESTRICCIÓN DE ACCESOS REMOTOS		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Durante la ejecución del plan de trabajo de Ubuntu en el servidor de Orfeo, se revisó el archivo " login.defs " y se verificó que existe la entrada "CONSOLE=/etc/console" pero se encuentra deshabilitada.	Se revisaran las observaciones y se aplicaran las que se consideren válidas, toda vez que el aplicativo ya no se encuentra en funcionamiento, solo está disponible para consulta.
ITEM	**RECOMENDACIONES**	
1	Evaluar la posibilidad de técnica de habilitar el parámetro "CONSOLE=/etc/console" con el fin de asegurar que el acceso directo del root solo se pueda realizar desde la consola.	

PLAN DE TRABAJO FIREWALL FORTIGATE 300C		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Identificamos debilidades en la detección de ataques en el firewall de la Supersolidaria.	Para atender esta observación estamos realizando los estudios previos para la adquisición de un FortiWeb
ITEM	**RECOMENDACIONES**	
1	Realizar periódicamente pruebas de hacking al firewall con el fin de evaluar las vulnerabilidades de este dispositivo.	

DEBILIDADES EN LA DEFINICIÓN DE ALERTAS Y ASEGURAMIENTO DE LOS PARÁMETROS DE APLICACIÓN		
ITEM	**HALLAZGO**	**RESPUESTA**
1	identificamos que no es posible la definición de alertas y aseguramiento de los parámetros de aplicación	Se van a hacer las validaciones respectivas con el proveedor
ITEM	**RECOMENDACIONES**	
1	Evaluar la viabilidad técnica de implementar mecanismos de hardware o software que permitan la configuración de alertas en el firewall, al igual que dispositivos que permitan definir los métodos de autenticación, implementación de IKE, métodos de cifrado o dead peer detection para reforzar la seguridad de las comunicaciones por VPN.	

PLAN DE TRABAJO DISPOSITIVO DE COMUNICACIÓN SWITCH CORE HP 5120		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Debilidades en la configuración de seguridad del switch de la Supersolidaria.	Se acepta y se revisará la implementación de estos parámetros.
ITEM	**RECOMENDACIONES**	
1	- Evaluar la viabilidad técnica de definir reglas en el switch que permita la restricción de accesos a usuarios de red. - Realizar la configuración del log en el switch y realizar revisiones periódicas a los mismos de forma que permitan identificar los incidentes o aspectos más relevantes en la red. - Evaluar la viabilidad técnica de deshabilitar el servicio de telnet**.**	

Objetivo 3:
Evaluación de las funciones críticas de tecnología de Información

DEFINICIÓN DE MÉTRICAS DE CUMPLIMIENTO E INDICADORES DEL ÁREA		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Conocimos por medio del Decreto 689 de 2005 las funciones definidas para la Oficina de Sistemas. Sin embargo identificamos que no se tienen métricas o indicadores	El citado Decreto no menciona en NINGUNO de sus apartes a la Oficina de Sistemas, por lo tanto no es coherente el hallazgo identificado. Se aclara además que el tema de indicadores de los gerentes públicos, se realiza a través de los denominados acuerdos de gestión y la de los funcionarios a través de la evaluación de desempeño para TODA la entidad.
ITEM	**RECOMENDACIONES**	
1	Diseñar e implementar mecanismos de medición de cumplimiento para las funciones críticas de tecnología, como indicadores de desempeño e indicadores de resultado.	

DEFINICIÓN DE ACUERDOS DE NIVEL DE SERVICIO CON LAS ÁREAS FUNCIONALES		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Los tiempos, configurados en la herramienta CA Service Desk Manager, en los cuales se deben atender las solicitudes e incidentes, son iguales independiente el tipo de requerimiento.	Se acepta y se solicitara la parametrización de los tiempos con la renovación del soporte del servicio.
ITEM	**RECOMENDACIONES**	
1	Definir e implementar tiempos de respuesta para cada uno de los tipos de incidentes y solicitudes configuradas en la herramienta, teniendo en cuenta los siguientes aspectos: - Complejidad del incidente o solicitud - Nivel de criticidad - Tiempo de respuesta por parte de la Oficina de Sistemas - Tiempo de respuesta por parte de terceros o proveedores (cuando aplique)	

ENCUESTA PARA MEDIR EL GRADO DE SATISFACCIÓN DE LOS USUARIOS CON LOS SERVICIOS DEL ÁREA DE TECNOLOGÍA		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Identificamos que la mayor cantidad de tipos de incidentes están relacionados con el soporte a nivel de los equipos de cómputo y soporte a nivel de hardware.	Se acepta. Se han realizado múltiples actividades para mejorar la interacción entre los usuarios y la Oficina. Se dará continuidad a este proceso para el satisfacción del usuario final

ITEM	RECOMENDACIONES
1	Con base en los resultados de la encuesta, se recomienda evaluar la posibilidad de: - Establecer actividades que permitan disminuir la cantidad de incidentes relacionados con soporte a nivel de equipos de cómputo y a nivel de hardware. Entre las actividades que se pueden realizar están las capacitaciones periódicas a los usuarios sobre el manejo de equipos de cómputo, realización de campañas de sensibilización sobre el uso y cuidado de los mismos y generar un repositorio de preguntas frecuentes relacionadas con los incidentes o solicitudes más comunes que puedan ser consultadas por los usuarios. - Incluir dentro del procedimiento de gestión de incidentes los tiempos de respuesta estimados para atender las solicitudes e incidentes. Realizar campañas para socializar el procedimiento y que los usuarios conozcan los tiempos estimados de respuesta a sus solicitudes. - Realizar campañas de sensibilización que permitan aumentar el uso de la herramienta CA Service Desk Manager por parte de los usuarios, para así poder llevar la trazabilidad y debida gestión del área de soporte a cada uno de los requerimientos realizados por los funcionarios. - Analizar las sugerencias dadas por los usuarios para fortalecer la interacción entre la Oficina de Sistemas y sus áreas y ver la posibilidad de ser tenidas en cuenta con el fin de mejorar los servicios brindados por el área.

Objetivo 4:

Diagnóstico sobre la administración de las bases de datos de la Superintendencia de la Economía Solidaria.

DOCUMENTACIÓN PARA LA CONFIGURACIÓN DE BASES DE DATOS		
ITEM	**HALLAZGO**	**RESPUESTA**
1	La Supersolidaria no cuenta con una política de creación, administración y custodia de los súper usuarios en los sistemas de información y bases de datos de la Supersolidaria.	Se aceptan los hallazgos, se documentará la información requerida para dar cumplimiento a lo solicitado.
2	No se cuenta con un estándar de configuración de bases de datos, que defina los lineamientos de configuración y seguridad de todas las bases de datos de la entidad	Se aceptan los hallazgos, se documentará la información requerida para dar cumplimiento a lo solicitado.

ITEM	RECOMENDACIONES
1	- Definir e implementar una política con los lineamientos a tener en cuenta para la creación, administración y custodia de súper usuarios y usuarios genéricos en los sistemas de información y bases de datos de la Supersolidaria. - Definir e implementar un estándar de configuración para las bases de datos de la Supersolidaria, donde se especifiquen los lineamientos de configuración y seguridad que incluyan por lo menos la siguiente información: - Parámetros de contraseñas - Políticas de auditoría - Revisión periódica de logs de auditoría: eventos a analizar, responsables, tiempo de retención de logs. - Configuración de servicios. - Actividades de mantenimiento de la base de datos

PLAN DE TRABAJO DE SEGURIDAD DE LA BASE DE DATOS ORFEO		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Existen varios usuarios con rol DBA para realizar las tareas de Backus en la base de datos. Además existen usuarios de pruebas en la base de datos de producción con altos privilegios	Se evaluaran los usuarios señalados y las recomendaciones, para realizar las validaciones y ajustes pertinentes.
2	Identificamos que hay usuarios que no han cambiado la contraseña por defecto.	Se evaluaran los usuarios señalados y las recomendaciones, para realizar las validaciones y ajustes pertinentes.
3	Identificamos que se tienen configurados parámetros para los perfiles de la base de datos los cuales no cumplen con las buenas prácticas de seguridad.	Se evaluará cuáles parámetros se podrán configurar de acuerdo a la políticas de la entidad que se establezcan.
4	Identificamos que los log de auditoría se encuentran activos. Sin embargo, no se realiza una revisión de los mismos	Se acepta. Se incluirá en la política de seguridad.
ITEM	**RECOMENDACIONES**	
1	**Usuarios con rol DBA en la base de datos Orfeo:** - Evaluar la viabilidad técnica de centralizar en un solo usuario la realización de copias de respaldo en la instancia de la base de datos de Orfeo. - Definir medidas para el manejo y custodia de usuarios de pruebas con altos privilegios en las bases de datos de producción de Orfeo.	
2	**Usuarios de la base de datos Orfeo con contraseñas por defecto:** Realizar el cambio de las contraseñas por defecto de los usuarios identificados.	

ITEM	RECOMENDACIONES
3	**Debilidad en las políticas de contraseñas definidas en la base de datos Orfeo:** Evaluar la posibilidad de modificar los parámetros de contraseña mencionados anteriormente de acuerdo a las buenas prácticas de seguridad: • FAILED_LOGIN_ATTEMPTS=4 • IDLE_TIME=30 • PASSWORD_GRACE_TIME=3 • PASSWORD_LIFE_TIME=30 • PASSWORD_LOCK_TIME=UNLIMITED • PASSWORD_REUSE_MAX=3 • PASSWORD_REUSE_TIME=1 • SESSIONS_PER_USER=1
4	**Debilidades en la revisión de log de eventos de la base de datos** Realizar revisiones periódicas a los log de auditoría e identificar los eventos más relevantes. Se deben dejar soportes de dicha revisión para ser entregados a la coordinación o jefatura de planeación y sistemas y tomar las acciones necesarias.

PLAN DE TRABAJO DE SEGURIDAD DE LA BASE DE DATOS FÁBRICA DE REPORTES		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Identificamos que hay usuarios que no han cambiado la contraseña por defecto.	Se evaluaran los usuarios señalados y las recomendaciones, para realizar las validaciones y ajustes pertinentes
2	Identificamos que se tienen configurados parámetros para los perfiles de la base de datos los cuales no cumplen con las buenas prácticas de seguridad.	Se evaluará cuáles parámetros se podrán configurar de acuerdo a la políticas de la entidad que se establezcan.
3	Identificamos que los log de auditoría se encuentran activos. Sin embargo, no se realiza una revisión de los mismos.	Se acepta. Se incluirá en la política de seguridad.

ITEM	RECOMENDACIONES
1	**Usuarios de la base de datos Fábrica de Reportes con contraseñas por defecto** Realizar el cambio de las contraseñas por defecto de los usuarios identificados.
2	**Debilidad en las políticas de contraseñas definidas en la base de datos fábrica de reportes** Evaluar la posibilidad de modificar los parámetros de contraseña mencionados anteriormente de acuerdo a las buenas prácticas de seguridad: • FAILED_LOGIN_ATTEMPTS=4 • IDLE_TIME=30 • PASSWORD_GRACE_TIME=3 • PASSWORD_LIFE_TIME=30 • PASSWORD_LOCK_TIME=UNLIMITED • PASSWORD_REUSE_MAX=3 • PASSWORD_REUSE_TIME=1 • SESSIONS_PER_USER=1
3	**Debilidades en la revisión de log de eventos de la base de datos** Realizar revisiones periódicas a los log de auditoría e identificar los eventos más relevantes. Se deben dejar soportes de dicha revisión para ser entregados a la coordinación o jefatura de planeación y sistemas y tomar las acciones necesarias.

PLAN DE TRABAJO MySQL		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Identificamos que aún se encuentra activa la base de datos “test” en el motor de MySQL	La base de datos “test” fue eliminada.
2	Ejecutamos el parámetro cat /dev/null > ~/.mysql_history e identificamos que no se ha borrado el historial de comandos de la base de datos MySQL.	Se va a verificar el tema y se tendrá en cuenta en la política de seguridad.
ITEM	**RECOMENDACIONES**	
1	Evaluar la viabilidad técnica de realizar las siguientes implementaciones de seguridad: - Realizar la modificación del nombre de la cuenta root - Eliminar o bloquear los usuarios en blanco que son creados por defecto al instalar la base de datos. - Eliminar la base de datos “test” que son creadas por defecto al instalar el motor de la base de datos - Deshabilitar el parámetro cat /dev/null > ~/.mysql_history para que no sea almacenada información relevante como contraseñas en el registro de la base de datos.	

Objetivo 5:

Diagnóstico sobre las competencias del personal de planta y de contrato de prestación de servicios de apoyo a la gestión que maneja y ejecuta los recursos informáticos de la compañía

OPORTUNIDADES DE MEJORA IDENTIFICADAS EN EL DIAGNÓSTICO SOBRE LAS COMPETENCIAS DEL PERSONAL DE PLANTA Y DE CONTRATO PRESTACIÓN DE SERVICIOS DE APOYO A LA GESTIÓN QUE MANEJA Y EJECUTA LOS RECURSOS INFORMÁTICOS Jefe de la Oficina de Planeación y Sistemas		
ITEM	**HALLAZGO**	**RESPUESTA**
1	identificamos que entre los requisitos de estudio requeridos para este perfil, no se solicitan estudios de temas relacionados con gobierno de TI, seguridad de la información y/o arquitectura empresarial	Los temas relacionados con perfiles de los cargos de la Supersolidaria, corresponden a la Secretaria General. Se le traslado a las observaciones para que sean evaluados por la dependencia competente.
ITEM	**RECOMENDACIONES**	
1	Evaluar la posibilidad de incluir dentro de los requisitos de estudio y experiencia para este perfil los siguientes requisitos: - Conocimientos en temas de gobierno de tecnología de la información, seguridad de la información y arquitectura empresarial. - Experiencia laboral relacionada con temas de tecnologías de la información.	

OPORTUNIDADES DE MEJORA IDENTIFICADAS EN EL DIAGNÓSTICO SOBRE LAS COMPETENCIAS DEL PERSONAL DE PLANTA Y DE CONTRATO PRESTACIÓN DE SERVICIOS DE APOYO A LA GESTIÓN QUE MANEJA Y EJECUTA LOS RECURSOS INFORMÁTICOS Coordinador de Sistemas		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Identificamos que algunos conocimientos básicos que se están solicitando ya no se necesitan para el desempeño del trabajo.	Los temas relacionados con perfiles de los cargos de la Supersolidaria, corresponden a la Secretaria General. Se le traslado a las observaciones para que sean evaluados por la dependencia competente.
ITEM	**RECOMENDACIONES**	
1	Evaluar la posibilidad de modificar el manual de funciones de este perfil de la siguiente manera: - Actualizar los requerimientos de conocimientos básicos definidos para el cargo de forma que estén acordes a las necesidades actuales de la entidad frente a las funciones que se deben desempeñar. - Solicitar conocimientos o estudios relacionados con administración de las bases de datos Oracle con el fin de poder actuar como respaldo en caso de ausencia o terminación del contrato de servicios del contratista asignado a la administración de la misma.	

OPORTUNIDADES DE MEJORA IDENTIFICADAS EN EL DIAGNÓSTICO SOBRE LAS COMPETENCIAS DEL PERSONAL DE PLANTA Y DE CONTRATO PRESTACIÓN DE SERVICIOS DE APOYO A LA GESTIÓN QUE MANEJA Y EJECUTA LOS RECURSOS INFORMÁTICOS Administrador de las bases de datos Oracle		
ITEM	**HALLAZGO**	**RESPUESTA**
1	El perfil del administrador de la base de datos debería tener estudios relacionados con la administración de base de datos Oracle 11g teniendo en cuenta las obligaciones definidas en el contrato.	El administrador actual cuenta con la experiencia y el conocimiento de la base de datos existente, se evaluará en caso de requerir la contratación de un nuevo ingeniero para esta labor.
ITEM	**RECOMENDACIONES**	
1	Evaluar la posibilidad de solicitar dentro de los requisitos de estudio para este perfil una certificación relacionada con administración de seguridad y desempeño de bases de datos Oracle 11g.	

Objetivo 6:

Diagnóstico sobre los planes de contingencia de todos los sistemas de información con que cuenta actualmente la Superintendencia de la Economía Solidaria.

OPORTUNIDADES DE MEJORA IDENTIFICADAS EN EL DIAGNÓSTICO SOBRE LOS PLANES DE CONTINGENCIA DE TODOS LOS SISTEMAS DE INFORMACIÓN CON QUE CUENTA ACTUALMENTE SUPERSOLIDARIA Gobierno de continuidad		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Ausencia de un modelo de roles /equipos de continuidad	El plan de continuidad vigente contiene esta información, sin embargo es necesario actualizarla.
2	Ausencia de políticas corporativas que establezcan el marco de operación de los planes de continuidad.	El plan de continuidad vigente contiene esta información, sin embargo es necesario actualizarla.

ITEM	RECOMENDACIONES
1	**Ausencia de un modelo de roles /equipos de continuidad:** Definir e implementar un modelo de roles y equipos de continuidad con responsabilidades claramente definidas para operación normal, durante y después de un evento de contingencia. Es importante que cada funcionario con un rol asignado cuente con al menos un funcionario de respaldo. **Ausencia de políticas corporativas que establezcan el marco de operación de los planes de continuidad:** Definir e implementar políticas corporativas que incluyan la siguiente información que permita establecer el marco de operación de los planes de continuidad: - Metodología - Pruebas del Plan - Administración y control del modelo de continuidad - Continuidad de tecnología y de terceros

ANÁLISIS DE RIESGO		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Debilidades en la consideración de riesgos que afectan la continuidad del negocio.	Este hallazgo esta repetido con el 2.1 del objetivo 1 por cuanto se mantiene la misma respuesta: Se evaluara con el funcionario encargado la identificación de riesgos adicionales. (Humanos, ambientales, físicos y tecnológicos)
ITEM	**RECOMENDACIONES**	
1	Definir e implementar una metodología de análisis de riesgo que permita determinar el grado de exposición de la compañía a sufrir interrupciones en su operación. Dentro de este análisis se deben considerar factores de riesgo que pueden afectar la continuidad de las operaciones tales como los operacionales, estratégicos, legales, cumplimiento, ambientales o de reputación.	

ANÁLISIS DE IMPACTO AL NEGOCIO		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Identificamos las siguientes debilidades en la metodología de análisis de impacto al negocio: Se definieron RTO y RPO para la recuperación de las aplicaciones. Sin embargo, no es claro conocer si están alineados con los tiempos definidos a nivel de cada proceso. Además estos indicadores no han sido aprobados por la alta gerencia dado que el documento no ha sido oficializado a la fecha de la revisión. - No se han definido recursos mínimos para dar una operación mínima aceptable. - No se han definido las dependencias internas entre procesos de negocio y externas (terceros y proveedores) - No se han definido periodos críticos de operación - No se han definido funciones y personal clave - No se han definido registros vitales y/o documentos claves	El plan de continuidad vigente contiene parte de esta información, sin embargo se revisará y se evaluará si es necesario actualizarlo parcialmente.

ITEM	RECOMENDACIONES
1	1. Evaluar la posibilidad de revisar y ajustar la metodología de análisis de impacto al negocio teniendo en cuenta los siguientes aspectos: - Considerar en la definición de RTO y RPO las necesidades de cada uno de los procesos críticos de la Supersolidaria y que las áreas que dependen de dichos procesos participen en la definición de los RTO y RPO. - Identificar y definir los recursos mínimos necesarios para dar una operación mínima aceptable - Identificar y definir las dependencias internas y externas de los procesos clave de la Supersolidaria y que pueden afectar la continuidad de las operaciones - Identificar y definir los periodos críticos de operación que se presentan en la entidad, como por ejemplo los periodos de tiempo en los que envían información las entidades vigiladas. - Identificar y definir las funciones y personal clave que permitan la continuidad de las operaciones - Identificar y definir registros vitales y/o documentos claves que permitan a la Supersolidaria iniciar sus operaciones en periodo de continuidad. 2. Definir dentro de las políticas de la Supersolidaria la actualización del análisis de impacto al negocio cuando se presenten cambios en los objetivos estratégicos o en procesos relevantes de la entidad.

ESTRATEGIA DE CONTINUIDAD		
ITEM	**HALLAZGO**	**RESPUESTA**
1	La Superintendencia no posee estrategias de continuidad específicas para los siguientes escenarios descritos dentro del plan: - Fallas en el sistema de aire acondicionado. - Caída del controlador de dominio.	El plan de continuidad vigente contiene parte de esta información, sin embargo se revisará y se evaluará si es necesario actualizarlo parcialmente.
2	Debilidades en la alineación de los RTO y RPO con las estrategias de continuidad.	El plan de continuidad vigente contiene parte de esta información, sin embargo se revisará y se evaluará si es necesario actualizarlo parcialmente
3	No se han definido estrategias en función de los procesos de negocio.	El plan de continuidad vigente contiene parte de esta información, sin embargo se revisará y se evaluará si es necesario actualizarlo parcialmente
ITEM	**RECOMENDACIONES**	
1	**1- Debilidades en la definición de estrategias de continuidad** - Definir e implementar estrategias para eventos que pueden afectar la continuidad de las operaciones. - Evaluar la posibilidad técnica de implementar sistemas de respaldo del aire acondicionado. - Evaluar la posibilidad de contar con servidores externos a la entidad que permitan respaldar la caída de los servidores principales. Adicionalmente, se deben realizar copias de respaldo de los archivos de configuración y archivos del sistema de los servidores y elaborar procedimientos de configuración estándar de los mismos que permitan tenerlos disponibles en el menor tiempo posible. - Identificar y definir estrategias de continuidad de las operaciones para casos en los que no se pueda tener acceso a las oficinas principales de la Supersolidaria, ya que este evento puede afectar la continuidad de las operaciones de la entidad. 2- **Debilidades en la alineación de los RTO y RPO con las estrategias de continuidad** Revisar cada una de las estrategias de continuidad definidas, de forma que se asegure que estas cumplan con los tiempos establecidos en el análisis de impacto al negocio. **3- No se han definido estrategias en función de los procesos de negocio** Implementar estrategias de continuidad que estén en función de los procesos de negocio y que permitan recuperarlos de manera oportuna y apropiada de acuerdo a las necesidades de la compañía. Para cada una de estas estrategias, definir los escenarios cubiertos y no cubiertos por el plan de continuidad del negocio.	

DOCUMENTACIÓN DEL PLAN DE CONTINUIDAD		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Debilidades en la metodología de diseño y documentación	El plan de continuidad vigente es el primero que se aprueba en la Entidad, por lo que está sujeto a mejoramiento durante la evaluación del mismo.
2	Debilidades en la vinculación del plan de continuidad con el manejo de crisis y atención de emergencias.	El plan de continuidad vigente es el primero que se aprueba en la Entidad, por lo que está sujeto a mejoramiento durante la evaluación del mismo.
ITEM	**RECOMENDACIONES**	
1	**1- Debilidades en la metodología de diseño y documentación:** **Definir e implementar una metodología de diseño y documentación de planes de continuidad que incluya:** - Procedimientos para la activación, recuperación y retorno a la operación normal de las operaciones. - Cambios en las políticas y procedimientos durante la operación en continuidad con el fin asegurar la operación normal. - Actividades y procedimientos de copias de respaldo, necesarias para el inicio de las operaciones en continuidad. - Directorio de continuidad con las personas claves dentro del plan de continuidad del negocio. Adicionalmente, diseñar un árbol de llamadas para la activación de la contingencia - Actividades administrativas durante operación normal que permitan mantener el plan operativo y actualizado. **2. Debilidades en la vinculación del plan de continuidad con el manejo de crisis y atención de emergencias** Definir e implementar procedimientos que vinculen el plan de continuidad de la compañía con los grupos de manejo de crisis y atención de emergencias de la Supersolidaria.	

PLANES DE RECUPERACIÓN DE TECNOLOGÍA		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Debilidades en la documentación formal de los procedimientos de recuperación de tecnología.	Se van a evaluar y a definir en los planes de recuperación de tecnología de todos los sistemas de información de la Entidad.
ITEM	**RECOMENDACIONES**	
1	Definir e incluir en los planes de recuperación de tecnología de todos los sistemas de información de la compañía los siguientes aspectos: - Premisas o escenarios que cubre el plan de recuperación de tecnología - Lista de chequeo de los recursos mínimos requeridos para recuperar la plataforma tecnológica - Equipos de recuperación tecnológica y los funcionarios que los conforman. - Directorio de continuidad y árboles de llamadas para actividades de escalamiento de incidentes para la activación los DRP (Disaster Recovery Plan). - Actividades para la activación del plan, recuperación y retorno a la operación normal. - Documentación de soporte para la recuperación, como manuales de usuario y manuales de administración de la plataforma. - Actividades administrativas a ejecutar durante operación normal para mantener el plan operativo y actualizado.	

PRUEBAS		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Debilidades en la ejecución de pruebas a los planes de continuidad y de recuperación tecnológica	Se van a ejecutar pruebas a los planes que se definan o actualicen.
ITEM	**RECOMENDACIONES**	
1	Se debe asegurar que se realicen pruebas a los planes de continuidad y de recuperación tecnológica una vez sea firmado y aprobado el plan de continuidad de la Supersolidaria. Esto con el fin de asegurar que las actividades descritas en el plan permitan cumplir con los RTO y RPO definidos para recuperar los procesos de la entidad. De acuerdo con los resultados de las pruebas, se deben ajustar los planes de continuidad y de recuperación tecnológica. Adicionalmente, se debe asegurar que estos planes sean probados por lo menos una vez al año.	

ACTIVACIÓN DEL PLAN DE CONTINUIDAD		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Debilidades en el cumplimiento de los tiempos definidos en el plan de continuidad.	Hacen referencia puntualmente al tema del aire acondicionado, situación que se presentó debido a que no se contrató con las especificaciones establecidas por ésta dependencia, lo que generó la contingencia y las dificultades posteriores para contratar a un proveedor calificado para el arreglo, incremento los tiempos. El cumplimiento de un plan de mantenimiento para los equipos de tecnología, va a estar sujeto al cumplimiento de especificaciones establecidas por esta dependencia. No se plantea acción de mejora puesto que la oficina cumple con enviar los estudios técnicos oportunamente.
ITEM	**RECOMENDACIONES**	
1	Revisar las estrategias de continuidad definidas para el tipo de contingencia que se presentó e identificar los cambios que se deben realizar para asegurar que estas estrategias permitan garantizar el cumplimiento de los RTO y RPO definidos. Identificar las razones por las cuales no se ha realizado el retorno a la operación normal de los servicios y definir un plan de acción para dar continuidad a este proceso de retorno. Ajustar la documentación del plan de continuidad de Supersolidaria, de acuerdo con los análisis sugeridos.	

Objetivo 7:

Diagnóstico sobre el diseño, implementación y efectividad de los controles para la administración de la infraestructura tecnológica de Supersolidaria para los sistemas Fábrica de Reportes, Sigcoop y Orfeo.

ADMINISTRACIÓN DE USUARIOS		
ITEM	**HALLAZGO**	**RESPUESTA**
1	El formato creación, modificación, eliminación e inactivación de usuarios y roles no se encuentra incluido dentro del procedimiento de administración de usuarios.	Se va a actualizar el documento
2	La tabla de usuarios de la bases de datos de Fábrica de Reportes no tiene los campos de fecha de creación de usuarios, ni fecha de último ingreso	Se van a realizar los ajustes a la tabla.
3	Funcionarios de planta retirados durante noviembre de 2013 y octubre de 2014, se encuentran activos en las aplicaciones Orfeo, Fábrica de reportes y/o el controlador de dominio.	Se acepta. Se depurara los usuarios reportados en la observación.
ITEM	**RECOMENDACIONES**	
1	**Procedimiento de administración de usuarios:** Actualizar el procedimiento de administración de usuarios de forma que se incluyan todas las actividades que actualmente se ejecutan durante el proceso de creación de usuarios en los sistemas de información de Supersolidaria. Dentro del procedimiento se debe incluir el uso del formato "creación, modificación, eliminación e inactivación de usuarios y roles".	
2	**Debilidades en la administración de usuarios de fábrica de reportes y Orfeo:** **-** Se debe asegurar que para todas las creaciones de usuarios en las aplicaciones, se soliciten los soportes descritos en el procedimiento de administración de usuarios para garantizar que son creaciones solicitadas y aprobadas por personal autorizado. Dentro de los soportes solicitados, se debe asegurar el uso el formato de creación de usuarios. - Evaluar la viabilidad técnica de incluir en la tabla de usuarios de Fábrica de Reportes, los campos de fecha de creación, fecha de últimos ingreso y fecha de bloqueo de los usuarios para poder llevar un registro de la administración de los mismos.	
3	**Funcionarios retirados con usuarios activos en las aplicaciones:** **-** Realizar el bloqueo y eliminación de los empleados y contratistas retirados de Supersolidaria que tienen usuarios activos en las aplicaciones Orfeo, Fábrica de reportes y en el controlador de dominio. - Revisar la ejecución del procedimiento de eliminación de usuarios y verificar si hay inconsistencias en el diseño del proceso que estén generando que hayan usuarios retirados de la compañía sin ser eliminados después de tanto tiempo de no laborar en la empresa. - Realizar revisiones periódicas de los usuarios con el fin de identificar en las aplicaciones usuarios activos que están vinculados a funcionarios o contratistas.	

REVISIÓN DEL CENTRO DE CÓMPUTO PRINCIPAL		
ITEM	**HALLAZGO**	**RESPUESTA**
1	- Debilidades en los controles ambientales y de seguridad - Se identificó que si bien se cuenta con un sistema central de aire acondicionado, al momento de nuestra revisión no se encontraba en funcionamiento. - Pese a que se realizan mantenimientos preventivos para el sistema de aire acondicionado no se tienen definidas actividades contingentes que permitan mantener los canales fríos dentro del centro de datos. - Se cuenta con un sistema biométrico de huella para controlar el acceso. Sin embargo, en la revisión identificamos que se tiene deshabilitado y la puerta permanece abierta para mitigar la concentración de calor en el centro de datos	Este requerimiento ya fue atendido en el mes de diciembre, con un contrato de soporte y mantenimiento por un año.
2	- La medición de temperatura dentro del centro de datos se realiza con el visor de medición que viene incluido en el sistema de aire acondicionado, por lo cual actualmente no se lleva el seguimiento diario de la temperatura. - No se lleva una bitácora de acceso al centro de datos.	Se incluirá dentro de las políticas de seguridad
3	- Obtuvimos los soportes del mantenimiento de UPS y aire acondicionado solamente para los meses de noviembre de 2013 y septiembre de 2014 por lo que podemos identificar que no se está realizando un mantenimiento periódico a estos sistemas - No obtuvimos los soportes de mantenimiento del sistema automático de extinción de incendios - Se cuenta con CCTV a nivel general del edificio pero no se tiene una cámara dentro del centro de datos ni en las zonas de acceso al mismo.	Se van a iniciar los proceso de contratación
4	Se identifica que dentro del centro de cómputo principal se cuenta con medios magnéticos para la realización de copias de respaldo pero no se cuenta con un inventario de los mismos.	Se está realizando el levantamiento de inventario de Tecnología.
5	Debilidades en los controles de acceso en el centro de cómputo principal	Los usuarios relacionados corresponden a los encargados del servicio de vigilancia. Se incluirá las observaciones dentro de las políticas de seguridad
ITEM	**RECOMENDACIONES**	
1	**1. Debilidades en los controles ambientales y de seguridad:** **-** Asegurar que los controles ambientales tales como el aire acondicionado, se encuentre en funcionamiento y en óptimas condiciones para el buen desempeño de los equipos que se tienen en el centro de cómputo. - Asegurar que se realicen mantenimiento periódico a los equipos de aire acondicionado, UPS y el sistema automático de extinción de incendios con el fin de asegurar su funcionamiento. - Definir e implementar mecanismos de contingencia para fallos en los controles ambientales del centro de cómputo como el aire acondicionado con el fin de conservar los canales de aire frío que necesitan los equipos para su buen funcionamiento. - Asegurar que se cuenten con sistemas, alertas o mediciones manuales del control de temperatura en el centro de cómputo. - Definir e implementar el uso de una bitácora de acceso para registrar los accesos al centro de cómputo. Incluir dentro de la bitácora aspectos como: fecha de ingreso, nombre y firma de la persona que ingresa, nombre y firma de la persona autorizada para dar ingreso a los visitantes y motivo de la visita. - Asegurar que los controles de acceso tales como lector de huella o bitácoras de acceso al centro de cómputo estén funcionando y sean debidamente diligenciadas para garantizar que solo se permita el ingreso a personas autorizadas. - Evaluar la posibilidad técnica de incluir dentro del circuito cerrado de televisión al menos una cámara que permita monitorear los accesos al centro de cómputo. - Definir medidas para la señalización externa de los medios magnéticos y llevar un inventario de los mismos con el fin de tener un seguimiento de la ubicación de estas cintas	

ITEM	RECOMENDACIONES
2	**2. Debilidades en los controles de acceso en el centro de cómputo principal:** - Deshabilitar el acceso en la unidad biométrica a los usuarios que no se encuentran autorizados para el ingreso al centro de cómputo. Además se deben realizar revisiones periódicas a los accesos para identificar accesos no autorizados - Definir una política de acceso al centro de cómputo donde se definan las personas autorizadas para el ingreso a realizar actividades de operación, administración y mantenimiento dentro del centro de cómputo. Además se debe establecer los horarios de ingreso para el personal propio y de terceros. - Definir formatos de ingreso o extracción de información, recursos, hardware o medios magnéticos del centro de cómputo.

ADMINISTRACIÓN DE CAMBIOS EN LAS APLICACIONES		
ITEM	**HALLAZGO**	**RESPUESTA**
1	No se incluye información de la administración de cambios	Se incluirá dentro del procedimiento de cambios.
2	No hay soportes de los cambios realizados en fábrica de reportes y Orfeo.	El proveedor entrego la documentación con los cambios realizados en fábrica de reportes. Respecto a Orfeo, los cambios quedaron registrados en el informe del ingeniero desarrollador. Se va a implementar y dar cumplimiento a la política de control de cambios.
3	Implementación del capturador Siafcoop	No se acepta este hallazgo debido a que no se va a implementar.

ITEM	RECOMENDACIONES
1	**1. Procedimiento de administración de cambios.** Modificar el procedimiento de administración de cambios para las aplicaciones de Supersolidaria donde se incluyan los siguientes aspectos: - Tipificación de los cambios. - Valoración del cambio y análisis de impacto - Actividades del proceso: Solicitud, aprobación, desarrollo, pruebas, paso a producción, seguimiento. - Personal encardo de avalar los cambios a realizar. - Personal encargado de la implementación de los cambios. - Formatos de documentación tanto de solicitud, aprobación del cambio, pruebas, aprobación para paso a producción y seguimiento. - Documentación soporte, de acuerdo al tipo de cambio a realizar (Ej. Cambios de urgencia o proyectos). - Actividades adicionales que se deban considerar cuando los cambios son realizados por terceros. - Actividades adicionales que se deban considerar cuando se realicen cambios a los datos en las bases de datos.

ITEM	RECOMENDACIONES
2	**2. Soportes de control de cambios realizados en Fábrica de Reportes y Orfeo** -Se debe asegurar que para todos los cambios realizados a las aplicaciones, se soliciten los soportes descritos en el procedimiento de administración de cambios para garantizar que el impacto de las modificaciones realizadas hayan sido revisadas y aprobadas y cumplan con las necesidades de la compañía. -Se debe asegurar que todos los cambios realizados a las aplicaciones sean probados por los usuarios funcionales antes de pasar a producción. Es necesario para esto, definir qué tipos de pruebas se realizarán, quienes las ejecutarán y aprobarán.
3	**3. Implementación del capturador Siafcoop:** Asegurar que las actividades descritas en el cronograma sean ejecutadas de acuerdo lo planeado. Adicionalmente, establecer medidas o planes de acción frente a las actividades que presenta retrasos o demoras en su ejecución, de forma que se implementen acciones que permitan cumplir con el cronograma establecido.

COPIAS DE RESPALDO		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Debilidades en el procedimiento de ejecución de copias de respaldo a las bases de datos	Se actualizara el procedimiento de Backus de acuerdo a las observaciones realizadas.
2	Realización de copias de respaldo a otros componentes claves de la organización.	Se actualizara el procedimiento de Backus de acuerdo a las observaciones realizadas.
3	Ausencia de controles para la replicación en línea de las bases de datos	Se actualizara el procedimiento de Backus de acuerdo a las observaciones realizadas.

ITEM	RECOMENDACIONES
1	**Debilidades en el procedimiento de ejecución de copias de respaldo a las bases de datos:** - Definir e implementar dentro del procedimiento de generación de copias de respaldo información, la periodicidad de ejecución del Backus realizado a las bases de datos y el tiempo de retención de la información. - Definir e implementar formalmente actividades para la restauración de copias de respaldo de la base de datos. Tener en cuenta la realización de restauraciones periódicas con el fin de asegurar la integridad y disponibilidad de las copias realizadas. - Definir e implementar mecanismos para que se puedan custodiar y almacenar respaldos de información fuera de las instalaciones de la Supersolidaria.
2	**Realización de copias de respaldo a otros componentes claves de la organización:** Definir e implementar mecanismos que garanticen la realización de copias de respaldo de información a componentes claves de la entidad. Asegurar que estas copias de respaldo sigan las actividades y lineamientos descritos dentro del procedimiento de ejecución de backups.
3	**Ausencia de controles para la replicación en línea de las bases de datos:** - Definir e implementar actividades de recuperación de los servidores del centro de cómputo principal con el fin de asegurar el uso de la replicación en línea de los datos almacenados en la base de datos Oracle. - Definir e implementar un procedimiento para realizar copias de respaldo de las bases de datos diariamente, teniendo en cuenta que la frecuencia semanal con la que se realiza el Backus de la información, no permite asegurar que se pueda dar continuidad a las operaciones que dependen de esta información en caso fallo de los servidores del centro de cómputo alterno.

GESTIÓN DE INCIDENTES		
ITEM	**HALLAZGO**	**RESPUESTA**
1	No hay Análisis de incidentes reportados	Se va a generar una base de datos de conocimiento que incluya acciones y actividades para solucionar incidentes
2	Tickets sin resolver en la herramienta	Se va a depurar la verificar el estado real de los tickets para cerrar o dar trámite
ITEM	**RECOMENDACIONES**	
1	**Análisis de incidentes reportados:** - Realizar un análisis periódico de los incidentes reportados frecuentemente con el fin de generar una base de datos de conocimiento que incluya acciones y actividades para solucionar este tipo de incidentes y que permitan identificar la causa de su continua falla. - Evaluar la posibilidad de realizar capacitaciones a los usuarios con mayor número de reporte de incidentes con el fin de disminuir la cantidad de solicitudes realizadas por estos usuarios.	
2	**Tickets sin resolver en la herramienta:** Definir e implementar mecanismos para asegurar la solución de los incidentes y solicitudes dentro de los tiempos de nivel de servicio establecidos para la resolución de los casos registrados en la herramienta C.A Service Desk Manager.	

ADMINISTRADOR DE LA CONSOLA DE ANTIVIRUS		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Administración de la consola de antivirus	Se dio trámite a este hallazgo, instalando con el proveedor equipo por equipo el Antivirus.
ITEM	**RECOMENDACIONES**	
1	- Asegurar que todos los equipos de la Supersolidaria se encuentren cubiertos por la consola del antivirus y que tengan el agente actualizado. - Establecer actividades periódicas de revisión y actualización del agente de antivirus para los equipos que no cuentan con acceso constante a la red de Supersolidaria.	

Objetivo 8:

Diagnóstico de seguridad de Infraestructura Tecnológica mediante pruebas de Ethical Hacking .

DIAGNÓSTICO DE SEGURIDAD DE INFRAESTRUCTURA TECNOLÓGICA MEDIANTE PRUEBAS DE ETHICAL HACKING		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Posibilidad de ataque debido al agente SNMP	Se acepta y se evaluara la viabilidad de modificarlo.
2	El servidor remoto transmite tráfico o información sin cifrar	Se acepta y se evaluara la viabilidad de modificarlo.

ITEM	RECOMENDACIONES
1	**Configuración predeterminada del agente SNMP:** - Evaluar la viabilidad de deshabilitar el servicio SNMP. Si éste no es utilizado, se recomienda deshabilitarlo. - Configurar filtros de paquetes UDP entrantes al puerto del servicio SNMP en el dispositivo. - Cambiar la configuración predeterminada de la cadena de comunidad SNMP.
2	**El servidor remoto transmite tráfico o información sin cifrar:** - Deshabilitar el servicio Telnet en el switch y en vez de este utilizar un protocolo seguro (cifrado) de comunicación, tal como SSH.

ANÁLISIS DE VULNERABILIDADES PÁGINA WEB www.supersolidaria.gov.co		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Formulario HTML sin protección para ataques CSFR	Se está realizando el proceso de contratación de una herramienta WAF para evitar ataques de este tipo.
2	Método HTTP TRACE permitido	Se está realizando el proceso de contratación de una herramienta WAF para evitar ataques de este tipo.
3	Acceso público al archivo Robots.txt	Se realizaron los ajustes detectados
4	Directorio común disponible en el servidor	Se realizaron los ajustes detectados.
5	Divulgación de la versión del servidor	Se realizaron los ajustes detectados.
ITEM	**RECOMENDACIONES**	
1	**Formulario HTML sin protección para ataques CSFR:** - Evaluar la posibilidad de que la aplicación solo acepte solicitudes POST. - Limitar el tiempo de vida de las cookies de sesión - Usar una cookie secreta para el envío de solicitudes del usuario - Asegurar que no se cuenta con los archivos clientaccesspolicy.xml y crossdomain.xml, los cuales permiten el acceso no autorizado.	
2	**Método HTTP TRACE permitido:** Evaluar la viabilidad técnica y operativa de deshabilitar los métodos TRACE y TRACK en el servidor Web.	
3	**Acceso público al archivo Robots.txt :** Verificar que las secciones/directorios y archivos configurados en el archivo robots.txt se encuentren configurados los privilegios de acceso solo para usuarios autorizados, con el objetivo de evitar que un usuario remoto pueda obtener de forma no autorizada información confidencial o privada.	
4	**Directorio común disponible en el servidor:** - Evaluar la información contenida en los repositorios mencionados en la Observación con el fin de verificar que no se revele información crítica del negocio (p.e. código fuente de aplicaciones, información de cuentas de usuario, mecanismos de autenticación, esquema de solicitudes, entre otros). En caso de que haya información que no sea necesaria tener publicada en el servidor, se recomienda eliminarla del repositorio. - Verificar qué personal puede tener acceso al directorio y garantizar que solo los usuarios autorizados cuenten con los permisos necesarios para acceder a la información.	

ITEM	RECOMENDACIONES
5	**Divulgación de la versión del servidor:** Configurar la página de error en los directorios que no pueden ser accedidos, en la cual solo se observe el mensaje de prohibido el acceso o ruta no encontrada y no se revele información del servidor.

ANÁLISIS DE VULNERABILIDADES EN EL SERVIDOR DE LA PÁGINA WEB 190.144.247.19)		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Autenticación de usuarios sin cifrado.	Se está realizando el proceso de contratación de una herramienta WAF para evitar ataques de este tipo.
ITEM	**RECOMENDACIONES**	
1	**Autenticación de usuarios sin cifrado:** Las credenciales de los usuarios se consideran información confidencial por lo cual siempre deben de ser transferidas al servidor a través de una conexión cifrada (HTTPS).	

Objetivo 9:
Revisión del procedimiento de administración de licenciamiento de software

PROCEDIMIENTO DE ADMINISTRACIÓN DE LICENCIAS DE SOFTWARE		
ITEM	**HALLAZGO**	**RESPUESTA**
1	No incluye información relacionada con los siguientes aspectos: 1. Procedimiento para la adquisición de licencias. 2. Solicitud de instalación de software. 3. Actualización de licencias adquiridas. 4. Verificación de licencias instaladas contra las licencias adquiridas. 5. Actividades para el monitoreo y revisión del software no autorizado en los equipos de cómputo	1. Los procesos de contratación se rigen por la Ley 80 y decretos complementarios. La Entidad cuenta con un “Manual de Contratación” código D-CONT-002, en el que se establecen los requerimientos de acuerdo al proceso a adelantar. Actualmente se tiene el procedimiento R-GEIN-001 “Asesorar en la adquisición de equipos de tecnología” 2. Se cuenta con la herramienta mesa de ayuda a través de la cual se hace seguimiento. 3. Se hace de acuerdo con la necesidad y está relacionado con el proceso de contratación previamente citado. Actualmente se tiene el procedimiento R-GEIN-001 “Asesorar en la adquisición de equipos de tecnología”. 4. Actualmente se tiene el inventario de las licencias instaladas, el cual se actualizará con las que se Adquieran o actualicen en el futuro. 5. Esta actividad no se realiza debido a que actualmente se cuenta con la herramienta PCSecure que impide la instalación de software no autorizado.

ITEM	RECOMENDACIONES
1	**Procedimiento de administración de licencias de software:** Definir e implementar procedimientos que permitan tener un control del licenciamiento de software de la entidad que incluyan por lo menos la siguiente información: • Procedimiento para la adquisición de licencias. • Procedimiento para la solicitud de instalación de software • Actividades para realizar la comparación de las licencias instaladas contra las licencias adquiridas. • Procedimiento para la actualización del inventario de licencias adquiridas por Supersolidaria • Actividades para el monitoreo y revisión del software no autorizado en los equipos de cómputo de la entidad • Periodicidad de las revisiones y responsables

INVENTARIO DE SOFTWARE INSTALADO		
ITEM	**HALLAZGO**	**RESPUESTA**
1	No se cuenta con inventario de software instalado.	Actualmente se está realizando el levantamiento de la información del software instalado por equipo y ubicación.

ITEM	RECOMENDACIONES
1	- Definir e implementar un inventario que permita llevar un registro del software instalado en cada una de las estaciones de trabajo y servidores Windows y Linux, donde se incluya la siguiente información: - Nombre del equipo. - Modelo del equipo. - Responsable. - Acta de entrega del equipo al responsable. - Tipo de máquina (Física o Virtual) - Tipo de PC (PC o Servidor). - Software instalado - Evaluar la viabilidad técnica de realizar un escaneo periódico a la red de Supersolidaria, y evaluar que: - No existan equipos de cómputo que no se encuentren dentro del inventario. - El inventario de equipos se encuentre actualizado. - El software instalado corresponde al software autorizado.

SOFTWARE SIN LICENCIAMIENTO		
ITEM	**HALLAZGO**	**RESPUESTA**
1	Software sin licenciamiento	Se acepta, pero se aclara que en el 2014 se inició un proceso que se declaró desierto y este año se solicitó nuevamente la apertura del proceso mediante radicado 20151210003783 para la contratación de las licencias de software requeridas por la entidad.

ITEM	RECOMENDACIONES
1	- Realizar la adquisición de las licencias faltantes para los productos relacionados en la observación con el fin de cumplir con los requerimientos de software necesarios para la operación de la Supersolidaria. - Establecer mecanismos que permitan asegurar que dentro de la contratación a través de subasta inversa u otros sistemas, sean tenidas en cuenta dentro de la licitación las licencias requeridas para el funcionamiento de los equipos o sean adquiridas por la Supersolidaria.

4. Resumen de hallazgos aceptados con actividades pendientes de realizar

La Oficina de Control Interno de acuerdo con la respuesta dada por la Oficina Asesora de Planeación y Sistemas, solicita se le remitan las evidencias que permitan validar o verificar la implementación o cumplimiento de las mismas:

ITEM	OBJETIVO	HALLAZGO	RESPUESTA OFICINA PLANEACION Y SISTEMAS
1	OBJETIVO 1	No se cuenta con métricas o indicadores que permitan realizar un seguimiento al beneficio esperado de los proyectos que ya han sido ejecutados por la Oficina de Sistemas.	No se emite respuesta por parte de la OAPS
2	OBJETIVO 1	No se han contemplado otros factores de riesgo a los que puede estar expuesta la entidad asociados a los recursos, las operaciones, las aplicaciones y la infraestructura tecnológica	Se evaluara con el funcionario encargado la identificación de riesgos adicionales. (Humanos, ambientales, físicos y tecnológicos)
3	OBJETIVO 1	No se tiene un inventario de activos de información que permita identificar la clasificación de la información dentro de la entidad, los riesgos a los que se encuentran expuestos y los controles necesarios para mantener su integridad, disponibilidad y confidencialidad.	La segunda recomendación se acepta
4	OBJETIVO 1	La gran mayoría de los usuarios ha tenido problemas de disponibilidad con al menos una de las aplicaciones que utilizan. Revisamos y la mayoría presenta problemas con Orfeo.	Se revisarán las observaciones dentro del contexto de la entidad en el entendido de que la oficina ha establecido los lineamientos requeridos para hacer el levantamiento de las necesidades de los usuarios. Orfeo ya no se encuentra en producción.
5	OBJETIVO 2	No se cuenta con una política formal de contraseñas para la Supersolidaria	Se acepta y se actualizará el documento de Acuerdo Individual Manejo Información
6	OBJETIVO 2	Identificamos parámetros que no están alineados con las buenas prácticas de seguridad.	Aceptamos revisar la implementación de estos parámetros de acuerdo a la situación actual de la entidad.
7	OBJETIVO 2	Identificamos dos usuarios habilitados y que no tienen fecha de ingreso al sistema.	Se acepta. Se depurara los usuarios reportados en la observación.
8	OBJETIVO 2	Identificamos que las siguientes políticas de auditoría no están activas en el directorio activo	Se acepta. El controlador de dominio fue instalado recientemente y esta implementación hace parte de la siguiente etapa.
9	OBJETIVO 2	Identificamos que los siguientes grupos no tienen usuarios asignados: tty, disk, kmem, dialout, fax, voice, floppy, tape, audio, operator, src, shadow, utmp, video, sasl, staff, users, crontab, fuse, mlocate, ssh, winbindd_priv, netdev, rvm.	Se revisaran las observaciones y se aplicaran las que se consideren válidas, toda vez que el aplicativo ya no se encuentra en funcionamiento, solo está disponible para consulta.

ITEM	OBJETIVO	HALLAZGO	RESPUESTA OFICINA PLANEACION Y SISTEMAS
10	OBJETIVO 2	Durante la ejecución del plan de trabajo de Ubuntu en el servidor de Orfeo, revisamos los parámetros de contraseña en el servidor e identificamos lo siguiente: Parámetros Valor configurado Políticas de Supersolidaria LOGIN_RETRIES 5 intentos No definido LOGIN_TIMEOUT 60 segundos No definido PASS_MAX_DAYS 9999 días 35 días PASS_MIN_DAYS 0 días No definido PASS_MIN_LEN Este parámetro no se encuentra definido. No definido	Se revisaran las observaciones y se aplicaran las que se consideren válidas, toda vez que el aplicativo ya no se encuentra en funcionamiento, solo está disponible para consulta.
11	OBJETIVO 2	Evidenciamos que la variable “UMASK” se encuentra configurada en 22, lo cual no se encuentra de acuerdo a las mejores prácticas.	Se revisaran las observaciones y se aplicaran las que se consideren válidas, toda vez que el aplicativo ya no se encuentra en funcionamiento, solo está disponible para consulta.
12	OBJETIVO 2	Durante la ejecución del plan de trabajo de Ubuntu en el servidor de Orfeo, se revisó el archivo " login.defs " y se verificó que existe la entrada "CONSOLE=/etc/console" pero se encuentra deshabilitada.	Se revisaran las observaciones y se aplicaran las que se consideren válidas, toda vez que el aplicativo ya no se encuentra en funcionamiento, solo está disponible para consulta.
13	OBJETIVO 2	Identificamos debilidades en la detección de ataques en el firewall de la Supersolidaria.	Identificamos debilidades en la detección de ataques en el firewall de la Supersolidaria. Para atender esta observación estamos realizando los estudios previos para la adquisición de un FortiWeb
14	OBJETIVO 2	identificamos que no es posible la definición de alertas y aseguramiento de los parámetros de aplicación	Se van a hacer las validaciones respectivas con el proveedor
15	OBJETIVO 2	Debilidades en la configuración de seguridad del switch de la Supersolidaria.	Se acepta y se revisará la implementación de estos parámetros.
16	OBJETIVO 3	Los tiempos, configurados en la herramienta CA Service Desk Manager, en los cuales se deben atender las solicitudes e incidentes, son iguales independiente el tipo de requerimiento	Se acepta y se solicitara la parametrización de los tiempos con la renovación del soporte del servicio.
17	OBJETIVO 3	Identificamos que la mayor cantidad de tipos de incidentes están relacionados con el soporte a nivel de los equipos de cómputo y soporte a nivel de hardware	Se acepta. Se han realizado múltiples actividades para mejorar la interacción entre los usuarios y la Oficina. Se dará continuidad a este proceso para el satisfacción del usuario final
18	OBJETIVO 4	La Supersolidaria no cuenta con una política de creación, administración y custodia de los súper usuarios en los sistemas de información y bases de datos de la Supersolidaria	Se aceptan los hallazgos, se documentará la información requerida para dar cumplimiento a lo solicitado
19	OBJETIVO 4	No se cuenta con un estándar de configuración de bases de datos, que defina los lineamientos de configuración y seguridad de todas las bases de datos de la entidad	Se aceptan los hallazgos, se documentará la información requerida para dar cumplimiento a lo solicitado.

ITEM	OBJETIVO	HALLAZGO	RESPUESTA OFICINA PLANEACION Y SISTEMAS
20	OBJETIVO 4	Existen varios usuarios con rol DBA para realizar las tareas de Backus en la base de datos. Además existen usuarios de pruebas en la base de datos de producción con altos privilegio	Se evaluaran los usuarios señalados y las recomendaciones, para realizar las validaciones y ajustes pertinentes.
21	OBJETIVO 4	Identificamos que hay usuarios que no han cambiado la contraseña por defecto.	Se evaluaran los usuarios señalados y las recomendaciones, para realizar las validaciones y ajustes pertinentes.
22	OBJETIVO 4	Identificamos que se tienen configurados parámetros para los perfiles de la base de datos los cuales no cumplen con las buenas prácticas de seguridad.	Se evaluará cuáles parámetros se podrán configurar de acuerdo a la políticas de la entidad que se establezcan.
23	OBJETIVO 4	Identificamos que los log de auditoría se encuentran activos. Sin embargo, no se realiza una revisión de los mismos	Se acepta. Se incluirá en la política de seguridad.
24	OBJETIVO 4	Identificamos que hay usuarios que no han cambiado la contraseña por defecto.	Se evaluaran los usuarios señalados y las recomendaciones, para realizar las validaciones y ajustes pertinentes
25	OBJETIVO 4	Identificamos que se tienen configurados parámetros para los perfiles de la base de datos los cuales no cumplen con las buenas prácticas de seguridad.	Se evaluará cuáles parámetros se podrán configurar de acuerdo a la políticas de la entidad que se establezcan.
26	OBJETIVO 4	Identificamos que los log de auditoría se encuentran activos. Sin embargo, no se realiza una revisión de los mismos.	Se acepta. Se incluirá en la política de seguridad.
27	OBJETIVO 4	Ejecutamos el parámetro cat /dev/null > ~/.mysql_history e identificamos que no se ha borrado el historial de comandos de la base de datos MySQL.	Se va a verificar el tema y se tendrá en cuenta en la política de seguridad.
28	OBJETIVO 6	Ausencia de un modelo de roles /equipos de continuidad	El plan de continuidad vigente contiene esta información, sin embargo es necesario actualizarla.
29	OBJETIVO 6	Ausencia de políticas corporativas que establezcan el marco de operación de los planes de continuidad.	El plan de continuidad vigente contiene esta información, sin embargo es necesario actualizarla.
30	OBJETIVO 6	Debilidades en la consideración de riesgos que afectan la continuidad del negocio.	Este hallazgo esta repetido con el 2.1 del objetivo 1 por cuanto se mantiene la misma respuesta: Se evaluara con el funcionario encargado la identificación de riesgos adicionales. (Humanos, ambientales, físicos y tecnológicos)

ITEM	OBJETIVO	HALLAZGO	RESPUESTA OFICINA PLANEACION Y SISTEMAS
31	OBJETIVO 6	Identificamos las siguientes debilidades en la metodología de análisis de impacto al negocio: Se definieron RTO y RPO para la recuperación de las aplicaciones. Sin embargo, no es claro conocer si están alineados con los tiempos definidos a nivel de cada proceso. Además estos indicadores no han sido aprobados por la alta gerencia dado que el documento no ha sido oficializado a la fecha de la revisión. - No se han definido recursos mínimos para dar una operación mínima aceptable. - No se han definido las dependencias internas entre procesos de negocio y externas (terceros y proveedores) - No se han definido periodos críticos de operación - No se han definido funciones y personal clave - No se han definido registros vitales y/o documentos claves	El plan de continuidad vigente contiene parte de esta información, sin embargo se revisará y se evaluará si es necesario actualizarlo parcialmente.
32	OBJETIVO 6	La Superintendencia no posee estrategias de continuidad específicas para los siguientes escenarios descritos dentro del plan: - Fallas en el sistema de aire acondicionado. - Caída del controlador de dominio .	El plan de continuidad vigente contiene parte de esta información, sin embargo se revisará y se evaluará si es necesario actualizarlo parcialmente.
33	OBJETIVO 6	Debilidades en la alineación de los RTO y RPO con las estrategias de continuidad.	El plan de continuidad vigente contiene parte de esta información, sin embargo se revisará y se evaluará si es necesario actualizarlo parcialmente
34	OBJETIVO 6	No se han definido estrategias en función de los procesos de negocio.	El plan de continuidad vigente contiene parte de esta información, sin embargo se revisará y se evaluará si es necesario actualizarlo parcialmente
35	OBJETIVO 6	Debilidades en la documentación formal de los procedimientos de recuperación de tecnología.	Se van a evaluar y a definir en los planes de recuperación de tecnología de todos los sistemas de información de la Entidad
36	OBJETIVO 6	Debilidades en la ejecución de pruebas a los planes de continuidad y de recuperación tecnológica	Se van a ejecutar pruebas a los planes que se definan o actualicen.
37	OBJETIVO 7	El formato creación, modificación, eliminación e inactivación de usuarios y roles no se encuentra incluido dentro del procedimiento de administración de usuarios	Se va a actualizar el documento
38	OBJETIVO 7	La tabla de usuarios de la bases de datos de Fábrica de Reportes no tiene los campos de fecha de creación de usuarios, ni fecha de último ingreso	Se van a realizar los ajustes a la tabla.

ITEM	OBJETIVO	HALLAZGO	RESPUESTA OFICINA PLANEACION Y SISTEMAS
39	OBJETIVO 7	Funcionarios de planta retirados durante noviembre de 2013 y octubre de 2014, se encuentran activos en las aplicaciones Orfeo, Fábrica de reportes y/o el controlador de dominio.	Se acepta. Se depurara los usuarios reportados en la observación.
40	OBJETIVO 7	La medición de temperatura dentro del centro de datos se realiza con el visor de medición que viene incluido en el sistema de aire acondicionado, por lo cual actualmente no se lleva el seguimiento diario de la temperatura. - No se lleva una bitácora de acceso al centro de dato	Se incluirá dentro de las políticas de seguridad
41	OBJETIVO 7	- Obtuvimos los soportes del mantenimiento de UPS y aire acondicionado solamente para los meses de noviembre de 2013 y septiembre de 2014 por lo que podemos identificar que no se está realizando un mantenimiento periódico a estos sistemas - No obtuvimos los soportes de mantenimiento del sistema automático de extinción de incendios -Se cuenta con CCTV a nivel general del edificio pero no se tiene una cámara dentro del centro de datos ni en las zonas de acceso al mismo.	Se van a iniciar los proceso de contratación
42	OBJETIVO 7	Se identifica que dentro del centro de cómputo principal se cuenta con medios magnéticos para la realización de copias de respaldo pero no se cuenta con un inventario de los mismos.	Se está realizando el levantamiento de inventario de Tecnología.
43	OBJETIVO 7	Debilidades en los controles de acceso en el centro de cómputo principal	Los usuarios relacionados corresponden a los encargados del servicio de vigilancia. Se incluirá las observaciones dentro de las políticas de seguridad
44	OBJETIVO 7	No se incluye información de la administración de cambios	Se incluirá dentro del procedimiento de cambios.
45	OBJETIVO 7	No hay soportes de los cambios realizados en fábrica de reportes y Orfeo.	El proveedor entrego la documentación con los cambios realizados en fábrica de reportes. Respecto a Orfeo, los cambios quedaron registrados en el informe del ingeniero desarrollador. Se va a implementar y dar cumplimiento a la política de control de cambios.
46	OBJETIVO 7	Debilidades en el procedimiento de ejecución de copias de respaldo a las bases de datos	Se actualizara el procedimiento de Backus de acuerdo a las observaciones realizadas.
47	OBJETIVO 7	Realización de copias de respaldo a otros componentes claves de la organización.	Se actualizara el procedimiento de Backus de acuerdo a las observaciones realizadas.

ITEM	OBJETIVO	HALLAZGO	RESPUESTA OFICINA PLANEACION Y SISTEMAS
48	OBJETIVO 7	Ausencia de controles para la replicación en línea de las bases de datos	Se actualizara el procedimiento de Backus de acuerdo a las observaciones realizadas.
49	OBJETIVO 7	No hay Análisis de incidentes reportados	Se va a generar una base de datos de conocimiento que incluya acciones y actividades para solucionar incidentes
50	OBJETIVO 7	Tickets sin resolver en la herramienta	Se va a depurar la verificar el estado real de los tickets para cerrar o dar trámite
51	OBJETIVO 8	Posibilidad de ataque debido al agente SNMP	Se acepta y se evaluara la viabilidad de modificarlo
52	OBJETIVO 8	El servidor remoto transmite tráfico o información sin cifrar	Se acepta y se evaluara la viabilidad de modificarlo
53	OBJETIVO 8	Formulario HTML sin protección para ataques CSFR	Se está realizando el proceso de contratación de una herramienta WAF para evitar ataques de este tipo
54	OBJETIVO 8	Método HTTP TRACE permitido	Se está realizando el proceso de contratación de una herramienta WAF para evitar ataques de este tipo.
55	OBJETIVO 8	Autenticación de usuarios sin cifrado	Se está realizando el proceso de contratación de una herramienta WAF para evitar ataques de este tipo.
56	OBJETIVO 9	No se cuenta con inventario de software instalado	Actualmente se está realizando el levantamiento de la información del software instalado por equipo y ubicación.
57	OBJETIVO 9	Software sin licenciamiento	Se acepta, pero se aclara que en el 2014 se inició un proceso que se declaró desierto y este año se solicitó nuevamente la apertura del proceso mediante radicado 20151210003783 para la contratación de las licencias de software requeridas por la entidad.

IV. Conclusiones y Recomendaciones

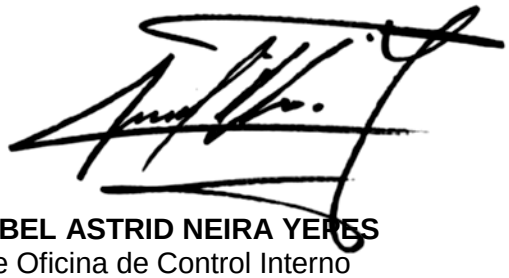
- ✓ De los setenta y nueve (79) hallazgos establecidos por la firma de auditoría Deloitte & Touche en los informes presentados sobre el diagnóstico integral de la plataforma tecnológica y sistemas de información de la Superintendencia de la Economía Solidaria, de acuerdo con la respuesta dada por la Oficina Asesora de Planeación y Sistemas, cincuenta y siete (57) fueron aceptados, nueve (9) no se aceptaron, once (11) fueron cumplidos, y dos (2) correspondían a acciones que debería realizar la Secretaria General de la Superintendencia.

- ✓ De conformidad con lo establecido en el punto 4 de este informe se solicita por parte de la Oficina de Control Interno a la Oficina Asesora de Planeación y

Sistemas remitir los documentos y soportes que permitan evidenciar las acciones realizadas.

- ✓ De igual forma se solicita informarnos si sobre los dos (2) hallazgos que corresponden a la Secretaria General, la Oficina Asesora de Planeación y Sistemas informo para que se implementaran las acciones y correctivos a que hubiera lugar.

Cordialmente,



MABEL ASTRID NEIRA YEPES
Jefe Oficina de Control Interno
Superintendencia de la Economía Solidaria

Elaboró BEATRIZ RANGEL MARTINEZ