INFORME DE AUDITORÍA

Código de auditoria: AUD-15108 Fecha: **Inicio** 2015-10-19 **Final** 2015-10-27

Fecha del informe: 2015-11-04

TIPO AUDITORIA	PROCESO, DEPENDENCIA O TEMA A AUDITAR	RESPONSABLE
Calidad	Gestión Tecnológica y de la Información	LUZ MARCELA RAMIREZ VELEZ

OBJETIVO

Evaluar el proceso de Gestión Tecnológica y de la Información, para verificar el cumplimiento de los requisitos especificados en la norma NTCGP 1000:2009, Modelo Estándar de Control Interno MECI, así como la normatividad vigente y los procedimientos establecidos para el proceso.

ALCANCE

Área responsable: Gestión Tecnológica y de la Información, se auditará este proceso durante el período comprendido entre el 01/04/2014 y el 30/09/2015, para esta auditoría se tendrá en cuenta la información publicada en el SIGER a la fecha de la auditoría. Verificación del cumplimiento y conocimiento de la caracterización, manual, instructivo, guías, formatos y demás documentos necesarios y procedimientos existentes.

CRITERIOS

Evaluar el cumplimiento de la normatividad definida en el normograma del proceso (leyes, decretos, resoluciones y acuerdos) y demás normatividad vigente, bajo la norma técnica de calidad en la Gestión Pública NTC GP 1000:2009. Igualmente son criterios de auditoría la caracterización del proceso y demás documentos como (procedimientos, instructivos, manuales y documentos externos).

AUDITOR LÍDER / DEPENDENCIA

GIOVANNI ARTURO GONZALEZ ZAPATA

EQUIPO AUDITOR

GLORIA AIDE GONZALEZ ALMARIO *

HALLAZGOS

1 Tipo Hallazgo: No conformidad

Descripción: De acuerdo al análisis de la base de datos de backup diarios proporcionada por Gestión Tecnológica y de la Información se evidenció que no se tiene registro diario del mes de abril incumpliendo el numeral 4.2.4 control de registros de la NTCGP1000

2 Tipo No conformidad

	Hallazgo:	
	Descripción:	De acuerdo al análisis de la base de datos de backup mensual proporcionada por Gestión Tecnológica y de la información se evidenció que el registro del backup del mes de marzo de 2015 se realizó el día lunes 6 de abril de la presente anualidad incumpliendo el numeral 5.3.2 respaldo de la información del manual del sistema de gestión de la seguridad de la Información – SGSI, el cual enuncia lo siguiente: Backup Mensual: Corresponde a la copia mensual completa en cinta de la información y el resultado se registra a través de la herramienta de automatización de la tarea. La copia se realiza el primer día hábil de cada mes
3	Tipo Hallazgo:	No conformidad
	Descripción:	Revisada la Política de control de accesos, numeral 5.4.1 “cuando un colaborador termina su relación laboral, sus permisos de acceso deberán ser revocados de forma inmediata” de acuerdo a la entrevista realizada al grupo coordinador de gestión Tecnológica y de la Información, se tiene establecido el procedimiento con Talento Humano, de informar en forma inmediata a gestión Tecnológica y de la Información, la novedad de personal “retiro” pero con el caso del Funcionario Javier Alonso Cárdenas Díaz, se evidenció que dicho procedimiento no se está cumpliendo por parte de Talento Humano, incumpliendo el procedimiento TH-P-05 desvinculacion de personal numeral 7 que enuncia: Enviar novedades de personal a jefes - Enviar correo electrónico a los responsables de las siguientes dependencias y/o grupos, informando la novedad de retiro del funcionario para hacer seguimiento a:... .Tecnología de la información: Desactivación de cuentas a Jefe de Oficina De Tecnologías de la Información y al correo soporteacr@acr.gov.co.
4	Tipo Hallazgo:	No conformidad
	Descripción:	Revisada la Política de control de accesos, numeral 5.4.1: cuando un colaborador termina su relación laboral, sus permisos de acceso deberán ser revocados de forma inmediata y de acuerdo a la entrevista realizada al grupo coordinador de gestión Tecnológica y de la Información, se evidenció el área de gestión Contractual no tiene establecido el procedimiento de informar en forma inmediata a gestión Tecnológica y de la Información, la novedad de (retiro) de los contratistas con terminación anticipada del contrato, incumpliendo el numeral 4.2.1 generalidades de la NTCGP:1000 literal c que enuncia: los procedimientos documentado.
5	Tipo Hallazgo:	No conformidad
	Descripción:	Verificado el Normograma del proceso de Gestión Tecnológica y de la Información se evidenció que se encuentra desactualizado, toda vez que no contempla la nueva versión del decreto 2573 de diciembre de 2014, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones incumpliendo el numeral 4.2.3 control de documentos de la NCTGP:1000 literal b que enuncia, revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.

DESARROLLO

El día jueves 22 de Octubre de 2015 a las 9:00AM. se realiza apertura de la auditoria de calidad al proceso de Gestión Tecnológica de la Información, en presencia de los siguientes colaboradores:
Dra Marcela Ramírez Vélez, Jaime Eduardo Santafe Patino, Andrea Fernández Ramírez y Brayan Gabriel Plazas R.

se continúa con la lista de chequeo:

1. Cuando fue la última actualización del nomograma?

Rta: En marzo de 2015, se debe cargar la última versión del decreto 2573.

No Conformidad: Verificado el Normograma del proceso de gestión Tecnológica y de la Información se evidenció que se encuentra desactualizado, toda vez que no contempla la nueva versión del decreto 2573 de diciembre de 2014, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones incumpliendo el numeral 4.2.3 control de documentos de la NTCGP:1000 literal B que enuncia, revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.
Caracterización:

1. evidenciar los informes de gestión producto establecido en la caracterización del proceso de gestión tecnológica y de la información y periodicidad

   Rta: Se realizó una presentación ante la alta dirección, esta semana se llevó a cabo seguimiento del informe, y dentro del proceso estratégico se encuentra la periodicidad.

Recomendación: de acuerdo a la entrevista realizada al jefe del proceso de Gestión Tecnológica y de la Información y su grupo asesor se recomienda establecer la periodicidad de los informes de gestión a cargo de dicho proceso.

1. Evidenciar los informes de cumplimiento de las políticas de seguridad informática del segundo semestre de 2014 y primer semestre de 2015.

   Rta: se está haciendo un análisis de brecha con respecto a la ISO:27001, y se han realizado 2 informes de análisis por recomendaciones del contratista toda vez que ellos deben entregar informes para mejorar la seguridad informática.

2. Evidenciar la Política de Seguridad de la Información?

   Rta: La política de Seguridad de la información se encuentra en el manual de Gestión de Seguridad de la información (SGSI) publicado en el SIGER.

Manual de Gestión de Seguridad de la Información (SGSI)

1. Con que periodicidad se realiza el inventario de activos de la información

Rta: se hace de forma permanente y justo ahora estamos en actualización de Activos de Información.

Observación: de acuerdo a la entrevista realizada al equipo coordinador de Gestión de Tecnológica y de la Información sobre la periodicidad en la actualización de activos de la Información, se evidenció que no se tiene establecida la periodicidad para

dicha actualización.

1. Cuando se definieron los procedimientos de rotulado, donde se encuentran documentados? Evidenciar.

Rta: se encuentran en fase de lineamientos una vez se encuentren aprobados se implementaran.

1. Evidenciar el registro de los Backup mensual, semanal y diario de noviembre de 2014 y julio de 2015

   Rta: se allega base de datos con el registro de los Backups diarios, semanales y mensuales.

   Observación Control Interno:
   En el backup diario no se encuentra el registro del mes de abril y en el Backup mensual, el registro del mes de marzo se realizó el día lunes 6 de abril de 2015.

No Conformidad: de acuerdo al análisis de la base de datos de backup diarios proporcionada por Gestión Tecnológica y de la Información se evidenció que no se tiene registro diario del mes de abril incumpliendo el numeral 4.2.4 control de registros de la NTCGP1000:2009

No Conformidad: De acuerdo al análisis de la base de datos de backup mensual proporcionada por Gestión Tecnológica y de la información se evidenció que el registro del backup del mes de marzo de 2015 se realizó el día lunes 6 de abril de la presente anualidad incumpliendo el numeral 5.3.2 respaldo de la información del manual del sistema de gestión de la seguridad de la Información – SGSI, el cual enuncia lo siguiente: "***Backup Mensual***: *Corresponde a la copia mensual completa en cinta de la información y el resultado se registra a través de la herramienta de automatización de la tarea. La copia se realiza el primer día hábil de cada mes.*

1. Que manejo, reportes y consecuencia conlleva los mensajes SPAM o Cadena mediante el correo institucional. Evidenciar casos.

   Rta: Se valida que el ataque sea personalizado o general, el sistema realiza un filtro y lo que no se logra filtrar los funcionarios realizan el reporte y se bloquea inmediatamente.

1. Allegar las cuentas deshabilitadas del segundo trimestre de 2015 y fecha cierta en las que se deshabilitaron y como se lleva el control?

   Rta: se tiene el procedimiento establecido donde Talento Humano realiza el reporte de la Información del personal que se retira de la ACR, a través de correo electrónico a gestión Tecnológica y de la Información y de forma inmediata se realiza el proceso de deshabilitar el respectivo usuario, con gestión Contractual no se tiene establecido procedimiento toda vez que automáticamente el sistema deshabilita la cuenta la fecha final del contrato.

   De la base de datos suministrada por Talento Humano, solicitada con anterioridad por el equipo auditor, de forma

aleatoria se seleccionan dos casos:

2. JAVIER ALONSO CARDENAS DIAZ retirado como funcionario de la Dirección General el 13 de enero de 2015 en forma voluntaria, el caso fue remitido por el mismo funcionario a Gestión Tecnológica y de la información a través de correo electrónico el día lunes 5 de enero de 2015. No se evidenció correo por parte de Talento Humano Informando el retiro del Funcionario para deshabilitar su cuenta de usuario.

3. MARTHA ROCIO ACEVEDO CONTRERAS retirada como funcionaria de la Secretaria General el 1 de Octubre de 2015, se evidenció el correo enviado por Talento Humano el día 29 de Septiembre de 2015 donde comunican a gestión Tecnológica y de la Información las novedades de personal solicitando el proceso de desvinculación de la misma.

No Conformidad: Revisada la Política de control de accesos, numeral 5.4.1 “cuando un colaborador termina su relación laboral, sus permisos de acceso deberán ser revocados de forma inmediata” de acuerdo a la entrevista realizada al grupo coordinador de gestión Tecnológica y de la Información, se tiene establecido el procedimiento con Talento Humano, de informar en forma inmediata a gestión Tecnológica y de la Información, la novedad de personal “retiro” pero con el caso del Funcionario Javier Alonso Cárdenas Díaz, se evidenció que dicho procedimiento no se está cumpliendo por parte de Talento Humano, incumpliendo el procedimiento TH-P-05 desvinculación de personal numeral 7 que enuncia " Enviar novedades de personal a jefes - Enviar correo electrónico a los responsables de las siguientes dependencias y/o grupos, informando la novedad de retiro del funcionario para hacer seguimiento a:... .Tecnología de la información: Desactivación de cuentas a Jefe de Oficina De Tecnologías de la Información y al correo soporteacr@acr.gov.co..."

No Conformidad: Revisada la Política de control de accesos, numeral 5.4.1 “cuando un colaborador termina su relación laboral, sus permisos de acceso deberán ser revocados de forma inmediata” de acuerdo a la entrevista realizada al grupo coordinador de gestión Tecnológica y de la Información, se evidenció que con gestión Contractual no se tiene establecido el procedimiento de informar en forma inmediata a gestión Tecnológica y de la Información, la novedad de “retiro” de los contratistas con terminación anticipada del contrato, incumpliendo el numeral 4.2.1 generalidades de la NTCGP:1000 literal c que enuncia "los procedimientos documentados"

1. Procedimiento de modificación de información contenida en el SIR (documentar)

   Rta: Se atiende como una solicitud o caso en el correo soporte ACR, se crea un ticket y se signa al personal competente del nivel central.

Procedimiento soporte a Usuarios – TI-P-02

1. Evidenciar formato TI-F-01 Formato solicitud de usuario o recurso tecnológico seguimiento y tiempos de respuesta.

   Rta: se allega el caso de Mónica Gómez Aparicio, solicitud enviada a través de correo electrónico por Diana Marcela Albarracín Núñez adjuntando formato de solicitud de usuarios y/o recursos tecnológicos TI-F-01, para creación de usuario y asignación de equipo portátil, con fecha de asignación al grupo el 17 de septiembre de 2015 a las 16:14 y se solucionó el día 18 de septiembre de la presente anualidad a las 17:03.

Procedimiento de Atención a Requerimiento de Sistemas de Información TI-P-01

1. Evidenciar un caso de requerimiento de sistema de información y allegar el acta de aceptación de la funcionalidad por el profesional de sistemas de información y el delegado de la dependencia solicitante paso 10 del procedimiento TI-P-01

Rta: se allegó el caso del Grupo de implementación sobre CU-SIR-CULMINACION-0001, realizando el control de cambios para quitar validación en terminación de beneficio de Salud y se evidencia el acta de culminación y terminación de beneficios firmada por la Coordinadora del Grupo de Implementación Katherin Díaz Albarracín y profesional Universitario de la Oficina de Tecnologías de la Información Hina Luz Garavito Robles.

OBSERVACIONES

De acuerdo a la entrevista realizada al equipo coordinador de Gestión de Tecnológica y de la Información sobre la periodicidad en la actualización de activos de la Información, se evidenció que no se tiene establecida la periodicidad para dicha actualización.

RECOMENDACIONES

CONCLUSIONES

ANEXOS

Anexo: INFORME AUDITORIA OTI.pdf