ALCALDÍA MAYOR DE BOGOTÁ D.C. INTEGRACIÓN SOCIAL Instituto para la Protección de la Niñez y la Juventud	PROCESO	AUDITORIAS INTERNAS	CODIGO	E-AUD-FT-003
	SUBPROCESO	AUDITORIAS INTERNAS	VERSIÓN	04
			PAGINA	1 de 4
	FORMATO	PLAN E INFORME DE AUDITORÍA	VIGENTE DESDE	21/08/2012

1. ETAPA DE PLANEACIÒN

PROCESO A AUDITAR:

PROCESO DE APOYO: TECNOLOGIAS DE INFORMACION Y COMUNICACIONES

EQUIPO AUDITOR

AUDITOR LIDER:	AUDITOR(ES) DE APOYO:
ARNULFO ALFREDO MEJIA ORTIZ	

AUDITADOS

CARGO	PERIODO PROGRAMADO PARA LA AUDITORIA		CARGO	PERIODO PROGRAMADO PARA LA AUDITORIA	
Dr. Gustavo de León Bonolis - Subdirector Técnico Administrativo y Financiero	DESDE: 29/05/2012	HASTA: 06/06/2012	Ing. Sonia Esperanza Amaya Torres - Responsable área de Sistemas.	DESDE: 29/05/2012	HASTA: 06/06/2012

OBJETIVO DE LA AUDITORÍA

El objeto de la auditoría interna es realizar la evaluación y seguimiento al proceso de apoyo a las tecnologías de Información y comunicaciones, verificando su funcionamiento, revisando el cumplimiento de la normatividad vigente, los principios de la administración pública y la implementación del SIGID, además de verificar la Integridad, confidencialidad y disponibilidad de los recursos y de la información.

ALCANCE DE LA AUDITORÍA

Verificar la adherencia del proceso de apoyo – Tecnologías de Información y comunicaciones-, a las normas constitucionales, legales, reglamentarias, y de autorregulación que les son aplicables, evaluando el desempeño de los sistemas informáticos y/o telemáticos así como el logro de los objetivos estratégicos.

Verificar las actividades relativas al proceso, con el fin de determinar el grado de economía, eficiencia y eficacia en el manejo de los recursos y los controles, de los métodos de medición e información sobre el impacto o efecto que producen los bienes y servicios entregados al cliente interno o partes interesadas.

Se utilizará entre otros el formato lista de chequeo código E-AUD-FT-004 para llevar a cabo la evaluación donde se establecen los puntos objeto de seguimiento, revisando documentación de las vigencias 2011 y 2012.

Este alcance aplica a los equipos del centro de cómputo, de interconexión de redes, aplicativos, bases de datos, sistemas operativos, estaciones de trabajo, portátiles, los datos, seguridad física, lógica y del entorno en las diferentes sedes del IDIPRON.

CRITERIOS DE AUDITORIA

1. Constitución Política de 1991	2. MECI 1000:2005	3.NTCGP 1000:2009
4. Directiva 005 de 2005	5. Resolución 305 de 2008	6. ISO/IEC 27002
7. ISO/IEC 27001	8. Acuerdo 308 de 2008 (Por el cual se adopta el Plan de Desarrollo Económico, Social, Ambiental y de Obras Públicas para Bogotá, D. C., 2008 – 2012 "BOGOTÁ POSITIVA: PARA VIVIR MEJOR")	9. PROCEDIMIENTO ASIGNACIÓN DE SOFTWARE - HARDWARE
10. PROCEDIMIENTO DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE SOFTWARE Y HARDWRE	11. PROCEDIMIENTO DESARROLLO Y ACTUALIZACIÓN DE SOFTWARE	12. PROCEDIMIENTO SOPORTE TECNICO

2. ETAPA DE EJECUCIÓN

RESUMEN DEL PROCESO DE AUDITORIA

La auditoria inicia dando cumplimiento al Programa de Auditoria para la vigencia 2012, aprobado por el Comité de Coordinación del Sistema de Control Interno mediante Acta Nª 20, del 5 de marzo de 2012.
Se realizó revisión y verificación del cumplimiento de los procedimientos asociados al proceso de apoyo "Tecnologías de Información y Comunicaciones", así como de la Resolución 305 de 2008, con especial énfasis en las políticas y gestión de seguridad de la información en la entidad.
Se visitaron las siguientes sedes: Aministrativa Cl. 63, Proyecto 4021, UPI (s) San Francisco, Eden, La Florida y LunaPark, sobre las cuales se tomó registro fotográfico de las condiciones físicas de seguridad y medio ambiente.

3. RESULTADOS DE LA AUDITORÍA

ASPECTOS POR RESALTAR Y MEJORAS EVIDENCIADAS

El IDIPRON goza de una infraestructura tecnológica de informática y de telecomunicaciones que le permite brindar servicios de Internet a las diferentes sedes y se dan las condiciones para que la población beneficiaria haga uso de estas herramientas para su formación y coadyuve a cumplir con su función misional.
-El personal del área de sistemas llega a involucrarse en el logro de los objetivos de la institución. Se han promovido acciones para buscar el mejoramiento continuo y dar cumplimiento a las necesidades o requerimientos del cliente interno.

Es muy importante revisar y confirmar la implantación del SGSI de acuerdo a la norma ISO/IEC 27001: 2005. Este sistema debe estar alineado al sistema integrado del IDIPRON -SGID- y a cada uno de sus componentes (NTCGP 1000:2009 "Norma Técnica de Calidad en la Gestión Pública ", MECI, 1000:2005 "Modelo Estándar de Control Interno para el Estado Colombiano " PIGA " Plan Institucional de Gestión Ambiental" y SIGA "Subsistema Interno de Gestión Documental y Archivos "). Igualmente, debe estar documentado y divulgado a todo el personal del IDIPRON. El SGSI permite gestionar de manera eficiente y confiable la información para preservar la integridad, confidencialidad y disponibilidad de la misma.

Se debe hacer una clasificación de la información y esta debe ser de acuerdo con el valor que le aporta al IDIPRON (Pública, privada, confidencial...etc.)

Se evidencian debilidades en cuanto a los sistemas automatizados que soportan la información administrativa y misional, por cuanto no responden a las necesidades de la entidad, si bien hay evidencias sobre la actualización y mejora de los módulos del software SYSMAN para la información administrativa y en cuanto al desarrollo del software a la medida para la información misional, aún no se cuenta con herramientas efectivas y con los atributos requeridos por la entidad.

El acceso al centro de cómputo mediante la utilización de técnicas biométricas (Huella digital), es una técnica acertada para un adecuado control de acceso. La existencia de cámara de video en el Data Center permite monitorear las acciones realizadas en la sala. Se cuenta con sistema de iluminación en el Data Center, que facilita la operación de los servidores y el mantenimiento de los mismos en el evento que falle el suministro público del fluido eléctrico; en cuyo caso se cuenta con equipos para soportar la emergencia como UPS y la planta eléctrica.

SEDE ADMINISTRATIVA: Cuenta con UPS y planta eléctrica de emergencia y sistema automático de transferencia, lo que garantiza la continuidad del fluido eléctrico y en consecuencia la continuidad de las operaciones o del servicio. Existe una adecuada conexión de los equipos de computo a la toma de tierra. Cuenta con breaker totalizador para la protección de acometida eléctrica de la red normal y regulada.

SEGURIDAD LOGICA: Se monitorea el acceso a la red y los recursos informáticos para protegerlo contra los abusos internos e intrusos externos. Se cambian periódicamente las claves. Se bloquean las claves de los ex funcionarios. A través del sistema operativo se exige no repetir las mismas claves y se garantiza que las claves sean robustas, no fácil de adivinar.

OBSERVACIONES Y RECOMENDACIONES

OBSERVACIONES

1. GESTION DE LA SEGURIDAD DE LA INFORMACIÓN - La Política de Seguridad del IDIPRON (Resolución 305 de 2008, art 16): El Manual de políticas básicas y especificas para manejo de la información del IDIPRON, se encuentra en proceso de actualización y durante la auditoría se pudo evidenciar que no existe un sito alterno para garantizar la continuidad de las operaciones o del servicio en caso de una contingencia y que igualmente sirva para la custodia de los medios de almacenamiento.

En el manual de política básica no se contempla la Seguridad ligada al Personal (Deben existir mecanismos de información y capacitación para los usuarios en materia de seguridad, así como de reporte de incidentes que puedan afectarla. Los servidores públicos deben cooperar con los esfuerzos por proteger la información y ser responsables de actualizarse en cada materia, así como consultar con el encargado de la seguridad de la información, en caso de duda o desconocimiento de un procedimiento formal, ya que esto no lo exonera de una acción disciplinaria que deba llevarse a cabo cuando se incurra en violaciones a las políticas o normas de seguridad.)

2. PLAN DE CONTINGENCIA (Resolución 305 de 2008, art 18): Las personas que conforman el equipo de contingencia no trabajan actualmente en el Instituto, tampoco corresponden algunos teléfonos de entidades de emergencia como es el caso de bomberos, ej. 2499297. El plan de contingencia no cuenta con un sitio alterno donde se pueda garantizar la continuidad de las operaciones o del servicio e incluso un sitio diferente al Data Center donde se custodien los datos de respaldo de la información ante una eventual falla o pérdida parcial o total de la información.
No existe presupuesto en el momento para contratar el sitio alterno para la continuidad de las operaciones o del servicio y la custodia de los medios de almacenamiento. No existe un procedimiento escrito de como restaurar una base de datos en Oracle con ninguna de las herramientas disponibles. Los equipos de red perimetral no se encuentran en alta disponibilidad con tolerancia a falla y redundancia en hardware.

3. SEGURIDAD FISICA (DATA CENTER - Resolución 305 de 2008, art 22 numeral 5): En la visita al Data Center se pudo evidenciar:
*Desechos de cables y partículas de polvo en el piso falso. *Cajas de cartón y rollo de papel contact. *Basura en el piso. * La puerta al data Center se encuentra obstruida por cestos de basura y cajas de papel para impresoras. *Falta de organización en el cableado en los rack. *El aire acondicionado en el momento de la visita se encontraba en observación por haberse presentado recalentamiento en los servidores , debido a estos inconvenientes no se está cerrando la puerta trasera del último rack, donde están los servidores , siendo la puerta una medita de protección. *Los cartuchos o las cintas que utiliza el "Data protector" para almacenamiento y recuperación de la información están visibles en el rack en lugar de guardarlas en el gabinete destinado para tal fin. (aquí se pierde la cadena de custodia).

4. SEGURIDAD FISICA DE LAS INSTALACIONES DE LA SEDE ADMINISTRATIVA: Resolución 305 de 2008, art 22 numeral 5): El cableado estructurado, concretamente el del centro de cómputo muestra desorden y mala presentación en los racks donde se encuentran ubicados los servidores, esta situación impide una rápida identificación y localización en el evento de posibles fallas o averías, impidiendo su pronta reparación.

Al aire acondicionado se requiere hacerle un monitoreo para garantizar que la temperatura preserve la seguridad e integridad de los servidores y demás equipos de Data Center.

5. CONTROL DE ACCESO A LOS DATOS - SEGURIDAD LOGICA - Resolución 305 de 2008, art 22 (dominio de control N. 7): Se pudo observar que en algunos computadores no se bloquea una sesión abierta, si esta se mantiene inactiva por mucho tiempo.

6. GESTIÓN DE ACTIVOS - Resolución 305 de 2008, art 22 (dominio de control N. 3) En visita a ciertas sedes del IDIPRON Av. Ciudad de Quito - 63 F - 35, Proyecto 4021, UPI La Florida, UPI Perdomo) se observaron equipos de cómputo en bodega; equipos que deberían revisarse o repararse para que sean utilizados en UPIs donde hagan falta, como es el caso de la UPI El Edén. No corresponde a la evidencia y a la norma señalada.

7. SEGURIDAD PERIMETRAL (DMZ) - SEGURIDAD FISICA - Resolución 305 de 2008, art 22, numeral 10 - GESTION DE LA CONTINUIDAD DEL NEGOCIO: El firewalls (corta fuego) no está en alta disponibilidad, en el evento de falla del equipo principal no existe otro que lo reemplace y permita la continuidad de las operaciones o del servicio con seguridad,

8. RED INALAMBRICA (WI-FI) - Resolución 305 de 2008, núneral 6 - GESTION DE LAS TELECOMUNICACIONES Y OPERACIONES: En el momento de la auditoría la red no estaba funcionando (31/05/2012, 2:40 pm.), esto se debió a que la red está en proceso de configuración en los Access point

9. COPIA DE SEGURIDAD BACKUPS - EMPRESA, GESTION DE COMUNICACIONES Y OPERACIONES - Resolución 305 de 2008, art 22, numeral 6: En el momento de la auditoría se solicitó procedimiento por escrito para la restauración de información, se manifestó que no existía.

RECOMENDACIONES

10. GESTION DE LA SEGURIDAD DE LA INFORMACIÓN - La Política de Seguridad del IDIPRON - Resolución 305 de 2008, art 16: La Política de Seguridad debe contemplar al menos la realización de un análisis de riesgos, procedimientos, la definición del plan de contingencia ante desastres; ese análisis de riesgos implica determinar lo siguiente: Qué se necesita proteger, quién debe protegerlo y cómo protegerlo. El manual de políticas debe incluir el uso adecuado de la red wi-fi , Red Privada Virtual y también de otros dispositivos de seguridad perimetral tal como el Sistema de Prevención de Intrusos.

Se recomienda una política de seguridad bien definida y divulgada en todos los niveles de la organización, que manifieste lo que está y lo que no está permitido en las redes.

11. PLAN DE CONTINGENCIA - Resolución 305 de 2008, art 18: Se recomienda adoptar políticas de seguridad , que permitan la custodia de la información, así como establecer los procedimientos para el adecuado uso y administración de los recursos informáticos. Para tal propósito se debe elaborar un documento actualizado y divulgarlo a todas las dependencias del IDIPRON acorde a la normatividad vigente en el ámbito Distrital, nacional e internacional.

12. SEGURIDAD FISICA (DATA CENTER - Resolución 305 de 2008, art 22 numeral 5: Se recomienda tener salas de cómputo seguras para la administración, almacenamiento y procesamiento de la información, se debe contar con protecciones físicas y ambientales que permitan preservar la integridad y disponibilidad de la información y de los recursos informáticos, organización del cableado y condiciones ambientales adecuadas .

Se recomienda organizar los cables en los rack y en lo posible cerrar el rack, previamente se resuelva el inconveniente con el aire. Igualmente se recomienda etiquetar los servidores.

13. ORGANIZACIÓN DE LA INFORMACIÓN - GESTION DE INCIDENTES DE SEGURIDAD - Resolución 305 de 2008, art 22 (dominio de control N. 9): Se recomienda establecer procedimientos de manejo de incidentes para garantizar una respuesta rápida, eficaz y sistemática de los incidentes de seguridad. Puesto que el identificar las fallas mas recurrentes permite afrontar mejor las causas de estos y respondiendo eficaz y oportunamente a la solución. Se requieren procedimientos bien documentados para que proceda el personal de soporte y mantenimiento si se detecta algún incidente de seguridad.

14. ORGANIZACION DE LA INFORMACIÓN - GESTION DE ACTIVOS - Resolución 305 de 2008, art 22 (dominio de control N. 7): Se recomienda clasificar la información para indicar la necesidad, las prioridades y el grado esperado de protección al manejar la información. Se debe realizar un análisis y valoración de la información manejada por el IDIPRON para definir una clasificación apropiada, dependiendo de su valor, sensibilidad e importancia.

15. CORREO ELECTRONICO - Resolución 305 de 2008, art 24, anexo 3: Según las recomendaciones y mejores prácticas que deben tenerse en cuenta para establecer un adecuado patrón de uso de los servicios de Correo Electrónico y de Acceso a Internet se sugiere insertar una cláusula de confidencialidad al final del correo institucional. (En el ítem "t" de la Política de seguridad menciona tal clausula , "Todo correo saliente debe llevar el siguiente pie de página de manera automática que será configurado por el Área de Sistemas".) USO GENERAL DEL CORREO INSTITUCIONAL En el ítem g registra lo siguiente: "Cada uno de los clientes deberá estar soportado por una licencia de correo." --En el Manual de política básica en el punto 4. (RESPONSABILIDAD DE LOS DIRECTIVOS) en el ítem a) dice: "Garantizar que todo el software usado por los empleados bajo su supervisión está propiamente licenciado. "

16. SEGURIDAD LOGICA - Resolución 305 de 2008, anexo 3: Según las recomendaciones y mejores prácticas que deben tenerse en cuenta para establecer un adecuado patrón de uso del Acceso a Internet se recomienda incluir una declaración acerca de cuáles son las obligaciones del usuario que va a trabajar con los recursos del sistema informático: impedir que otros usuarios puedan utilizar la misma sesión, no compartir su contraseña, no copiar o revelar datos confidenciales. Asimismo, en dicho mensaje se le debe advertir que el IDIPRON podrá registrar la actividad del usuario en los "logs" del sistema por motivo de seguridad.

Se recomienda que en todos los equipos después de 5 minutos de inactividad se bloquee el terminal, esto con el fin de evitar suplantadores que aprovechan sesiones abiertas. Algunos sistemas operativos permiten que al momento de logearse al sistema se advierta al usuario cual fue su última conexión, esto ayuda a evitar posibles suplantaciones.

17. SEGURIDAD PERIMETRAL (DMZ) - SEGURIDAD FISICA - Resolución 305 de 2008, art 22, numeral 10 - GESTION DE LA CONTINUIDAD DEL NEGOCIO: Se recomienda considerar que para preservar la seguridad de la información se requiere la disponibilidad de recursos y de información. Se debe actualizar la política de seguridad teniendo en cuenta las reglas de control de acceso con los equipos que forman parte de la red perimetral (firewalls, IDS, IPS, etc.)

18. RED INALAMBRICA (WI-FI) - Resolución 305 de 2008, núméral 6 - GESTION DE LAS TELECOMUNICACIONES Y OPERACIONES: Se recomienda proteger que la señal no trascienda los limites del edificio para que no sea interceptado por personal no autorizado. La red Wi-Fi se sugiere que forme parte de la política de seguridad.

19. COPIA DE SEGURIDAD BACKUPS - EMPRESA, GESTION DE COMUNICACIONES Y OPERACIONES - Resolución 305 de 2008, art 22, numeral 6: Se recomienda documentar el procedimiento que garantice la restauración de la información, la salvaguarda de los recursos informáticos y/o telemáticos, cuyo fin esencial es garantizar la continuidad de las operaciones y del servicio.

NO CONFORMIDADES LEVANTADAS

NC No.	DETALLE
1	La Política de Seguridad no se encuentra actualizada y ampliamente difundida en todo el Instituto, incumpliendo lo establecido en el Artículo 16 de la Resolución 305 de 2008.
2	El área de sistemas no cuenta con un Plan de Contingencia actualizado, que garantice la continuidad del servicio y/o operaciones ante un desastre causado por la naturaleza o por el hombre, incumpliendo el artículo 18 de la Resolución 305 de 2008.
3	La seguridad física del Data Center no está garantizada en razón a que el ambiente y las condiciones del salón no son las adecuadas por partículas de polvo existentes en el piso falso y en la misma superficie del centro, de igual forma la administración del cableado en los racks no cumple con la normatividad existente a nivel nacional e internacional, Resolución 305 de 2008 en el Artículo 22, numeral 5, así como en la norma internacional ISO/IEC 27002 en el Dominio de control No. 9.
4	No se cuenta con un sistema para manejo de incidentes de seguridad de la información, ni se registran los problemas recurrentes, incumpliendo el numeral 9 del artículo 22 de la Resolución 305 de 2008.
5	No se evidenció procedimiento documentado para respaldo y recuperación de la información, incumpliendo el articulo 22 numeral 6 de la Resolución 305 de 2008 y la norma internacional ISO/IEC 27002 Dominio No. 10 GESTIÓN DE COMUNICACIONES.
6	No existe el SGSI, sistema donde se definen las directrices y lineamiento del Instituto, el cual debe estar alineado con el Sistema Integrado de Gestión-SGID-, en cada uno de sus componentes, esto es, (NTCGP 1000:2009 "Norma Técnica de Calidad en la Gestión Pública ", MECI, 1000:2005 "Modelo Estándar de Control Interno para el Estado Colombiano " PIGA " Plan Institucional de Gestión Ambiental" y SIGA "Subsistema Interno de Gestión Documental y Archivos "). Tal como se expresa en la Resolución 305 de 2008 en el Articulo 13.

FIRMA RESPONSABLE DEL PROCESO	FIRMA AUDITOR LIDER