ALCALDÍA MAYOR
DE BOGOTÁ D.C.
GOBIERNO SEGURIDAD Y CONVIVENCIA
Departamento Administrativo de la
Defensoría del Espacio Público

MEMORANDO

AL CONTESTAR CITE EST 20151E2454
Folios: Anexo:0 Tipo doc:MEMORANDO
DEFENSORIA ESPACIO PUBLICO 02-12-2015 03:44:06
ORIGEN : SDSS - OACI /VALDERRAMA GUTIERREZ WILLIAM
DESTINO: DESP /JIMENEZ GONZALEZ NELSON YOVANY
ASUNTO: INFORME FINAL DEL PROCESO DE EVALUACION DE LA SE
OBS : DIEGO URAZAN

PARA: NELSON YOVANY JIMENEZ GONZALEZ
Director

DE: WILLIAM VALDERRAMA GUTIERREZ
Jefe Oficina de Control Interno

Asunto: Informe Final del proceso de evaluación de la seguridad física en el ámbito tecnológico de la Entidad.

La Oficina de Control Interno en cumplimiento de su rol de evaluación y seguimiento y en ejercicio de sus funciones en especial las establecidas en la Ley 87 de 1993 y teniendo en consideración lo dispuesto en los artículos 1°,2°, 3°, 4° y 12 de la misma norma, también de la Directiva de la Alcaldía Mayor N 005 de 2005 respecto a las políticas generales de Tecnología de información y comunicaciones aplicables a las Entidades del Distrito Capital y la Resolución 305 de 2008 Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre, así como también basado en la norma NTC-ISO/IEC 27001 que establece los requisitos del Sistema de Gestión de Seguridad de la Información y NTC-ISO/IEC 27002 que establece las mejores prácticas para la implementación del Sistema de Gestión de Seguridad de la Información, realizó una evaluación respecto a la seguridad física en el ámbito tecnológico de la Defensoría, y basado en lo anterior a continuación se presentan las siguientes iteraciones:

I. OBJETIVO Y ALCANCE:

La evaluación tuvo como objetivo principal, la validación y evaluación de la seguridad física en referencia a la plataforma tecnológica de la Entidad.

El trabajo de campo se desarrolló en las instalaciones del DADEP que se encuentran en el edificio de catastro piso 15 y 16, así como también los puestos de atención al público y la oficina de correspondencia ubicados en el SUPERCADE de la 30. Finalmente, la labor de auditoria se realizó con la colaboración de la Oficina de Sistemas y Subdirección Administrativa y Financiera y de Control Disciplinario.

02 DIC. 2015
4:09 p.m.

Carrera 30 No. 25 – 90 Piso 15
Bogotá D.C. Código Postal 111311
PBX: 3822510
www.dadep.gov.co
Línea: 195

II. METODOLOGIA

Para el desarrollo de la evaluación, se realizó un requerimiento de información el cual fue respondido en óptimas condiciones de calidad y tiempo; las fuentes de información remitidas a esta Oficina en general fueron:

- Documento centro de cómputo.
- Fotografías del centro de cómputo anterior.
- Informe de panorama de riesgos.
- Programa de seguridad orden y limpieza.
- Estudio de seguridad DADEP 2015.

Las evidencias se tomaron por medio de muestreo, a las cuales se aplicación procedimientos de auditoria tales como consulta, análisis de datos, observación, inspección y confirmación.

III. ASPECTOS POSITIVOS Y FORTALEZAS

Ejecutada la labor de auditoría, a continuación se expresan los siguientes aspectos que permiten determinar y dimensionar la gestión de la Entidad en referencia a la seguridad física, así como también permitieron ser factores críticos de éxito para la evaluación:

- Las oficinas de DADEP cuenta con perímetros de seguridad física las cuales brindan protección a los componentes de la plataforma tecnológica y en general del recurso humano, permitiendo tener un adecuado resguardo de la información en la Entidad.
- Se tiene una señalización informativa a lo largo de las instalaciones, que permite guiar a colaboradores y visitantes durante su permanencia.
- El DADEP tiene diseñado y en operación un sistema de seguridad física para el ingreso por medio de controles en sus instalaciones como son guardas de seguridad, cámaras de video grabación, puertas con lectoras de carnet por proximidad y registros en bitácoras de acceso a visitantes.
- El centro de cómputo cuenta con unas condiciones ambientales y de seguridad adecuadas, ya que se han implementado controles tales como acceso por lector biométrico, aire acondicionado, cámara de seguridad, sistema de extinción de incendios, alarma manual de incendios, detectores de humo, piso falso, rejilla que independizan el cableado de datos del cableado eléctrico, bitácora para visitantes, entre otros.

- El estado del centro de cómputo se encuentra en óptimas condiciones de limpieza y orden para todos los elementos allí contenidos.
- Se cuenta con un cableado estructurado (eléctrico y datos) ordenado y debidamente marcado a lo largo de las instalaciones de la Entidad.
- Se tienen establecidas estrategias para garantizar que el personal autorizado dispone de acceso a las instalaciones de la Entidad. Así como también se tienen estrategias para la atención de visitantes y proveedores.
- Se tienen implementadas actividades para controlar la salida y entrada de equipos de cómputo de la Entidad y del edificio del CAD.
- Como protección de equipos respecto al suministro de energía, se tiene instalado un cableado eléctrico debidamente identificado y conectado al sistema de UPS, para una autonomía de corriente que permite un correcto guardado y cierre de equipos (pc´s y servidores) en caso de falla en el suministro eléctrico, caídas y picos de voltaje
- La actividad de administración y entrega de los carnet de identificación y tarjetas de proximidad se encuentra operando y al día para todos los funcionarios y contratistas.
- Los extintores distribuidos a los largo de las instalaciones del DADEP se encuentra debidamente cargados y todos ellos sin vencerse.
- Los requerimientos de información solicitados a las áreas auditadas fueron respondidos de manera inmediata evitando retrasos en el desarrollo de la auditoria.

IV. OBSERVACIONES Y RECOMENDACIONES

A continuación presentamos las observaciones derivadas del trabajo de auditoría que requieren una intervención por parte de las áreas auditadas por medio de un plan de mejoramiento:

1. Puertas de acceso a las instalaciones de DADEP:

Realizando recorrido por las instalaciones de la Defensoría, se observa que las 2 puertas de acceso (oriental y occidental) no están realizando su cierre completamente, según lo visualizado, el mecanismo de devolución de las puertas no está ejerciendo la suficiente fuerza para que esta llegue al electroimán quedando en la mayoría del tiempo mal asegurada.

Recomendaciones:

- Solicitar el proveedor y/o personal encargado de la planta física de la Entidad, la revisión y mantenimiento de las puertas de ingreso (oriental y occidental) a las instalaciones, con el fin principal de validar el funcionamiento del mecanismo de devolución de puertas para que estas realicen su cierre completamente y obligue a los funcionarios el uso del carnet de proximidad para todo instante.
- Dentro del plan anual de mantenimiento para la planta física incluir la revisión de las puertas de acceso.

2. Equipos de cómputo con usuario desatendido:

Se revisan los equipos de cómputo de la Oficina de Control Interno y al dejarlos un tiempo sin utilizar, se observan que 3 de estos no bloquean la sesión automáticamente después de 1 hora de hacer seguimiento; esto aplica para equipos nuevos y antiguos. Lo anterior quiere decir que no se está aplicando un control sobre la sesión de usuarios cuando estos se ausenten de su puesto de trabajo por un tiempo prolongado.

Recomendaciones:

- ✓ Dentro de la documentación del proceso de gestión de la información y la tecnología definir y adicionar un lineamiento que contenga el tiempo de bloqueo de equipos sin uso.
- ✓ Implementar y en caso de existir el control, aplicar para todas las maquinas conectadas a la red la función automática que permita el bloqueo de las estaciones después de un tiempo sin uso tal y como se estableció en el lineamiento.

3. Data Center

Durante la ejecución de la auditoría se realiza visita al centro de cómputo de la Entidad y como resultado se informan los siguientes aspectos:

- Lectores de humedad: No se evidencia un instrumento o mecanismo para le medición del nivel de humedad en el centro de cómputo; adicional se menciona que dentro de la guía de seguridad de la información oficializada en el SIG, se menciona que ..*"el límite de humedad no debe superar el 65% para evitar el*

deterioro".. Basado en esto no se posible conocer el porcentaje de humedad dentro del recinto actualmente.

- Elementos dentro del centro de cómputo: Se evidencian cajas de cartón con materiales electrónicos, equipos de cómputo para entrega y una botella de líquido dentro del centro de cómputo. Como aspecto importante se menciona que los equipos de cómputo observados se encuentran allí debido a que están en alistamiento y también porque la Oficina de Sistemas no cuenta con una bodega para su almacenamiento.

- Lectora biométrica. Al revisar el estado de la lectora biométrica para acceder el centro de cómputo, se observa que la carcasa se encuentra desprendida de su base y sostenida con unos elásticos. Este evento se presentó debido a que un funcionario venia desplazándose rápidamente y accidentalmente se chocó contra la lectora biométrica generando el daño; de acuerdo con la información suministrada por la Oficina de Sistemas, la lectora biométrica sigue operando correctamente pero que no se ha cambiado la carcasa debido a su alto costo según lo informado por el proveedor. Como complemento se menciona que la lectora biométrica tiene un modo de configuración sencillo, por tal razón no se puede conocer la actividad presentada con esta por medio de un log o registro de ingresos.

- Visualización al interior del centro de cómputo: De acuerdo con las buenas prácticas de la industria, un Data center es una área sensible y confidencial que no puede estar visible, ya que este es el corazón de la plataforma tecnológica de una Entidad, para tal fin, el interior del centro de cómputo en general, equipos, controles implementados y demás componentes pueden ser visualizados desde el exterior por cualquier visitante exponiendo lo contenido allí, además se resalta que por el frente del centro de cómputo queda el pasillo principal de la Entidad por donde hay tráfico constante de personal.

- Respecto a la bitácora para control de acceso al centro de cómputo, se observa que el día de la visita de auditoría (11 de noviembre de 2015) había presencia de un proveedor (Hasan-5) chequeando un tema eléctrico, sin embargo no se evidencia el registro de la visita de dicho personal en el formato. También, el día 23 de noviembre ingresaron a la Entidad personal de la SHD y el proveedor Hasan-5 con acompañamiento de personal de SAF y sistemas al centro de cómputo y no se evidencia el registro en la bitácora.

Recomendaciones:

- ✓ Validar la adquisición de unos medidores de humedad e instalarlos dentro del centro de cómputo con el fin de medir el grado y comportamiento de este factor dentro del recinto y así tomar correctivos correspondientes en caso de detectarse alguna variación importante del grado de humedad, para así evitar la afectación de los equipos y elementos allí contenidos. Lo anterior también permite cumplir con lo establecido en la guía de seguridad de la información de la Entidad.
- ✓ Diligenciar estricta y completamente el formato "control de acceso al centro de cómputo" cada vez que ingresa personal externo, proveedor y funcionario de DADEP al centro de cómputo.
- ✓ Llevar un registro periódico de los valores de temperatura y humedad para así detectar anomalías en estos aspectos ambientales y poder tomar los correctivos correspondientes.
- ✓ Depurar y despejar del centro de cómputo todos los elementos que no pertenezcan a este como pc´s, cargadores, cables, cajas y botellas.
- ✓ Solicitar vía memorando a la Subdirección Administrativa, Financiera y de Control Disciplinario sea asignado un espacio como bodega para la Oficina de Sistemas.
- ✓ Validar con el proveedor de la lectora biométrica para el centro de cómputo el cambio de carcaza, para que esta se encuentre en condiciones idóneas. Y para evitar situaciones similares, validar la opción de asegurar con una estructura que proteja la lectora.
- ✓ Realizar el análisis costo beneficio de instalar para la puerta y el vidrio del centro de cómputo una película opaca con el fin de evitar que el interior del centro de cómputo se pueda observar con claridad.
- ✓ Validar la reubicación del sensor de luz dentro del centro de cómputo a un punto central y adicional, validar la instalación de un switch que permita tener la luz encendida constantemente mientras se realicen trabajos al interior por parte de personal de la Entidad o proveedores externos.
- ✓ Realizar un análisis costo beneficio para la instalación de un detector de humo encima del techo y debajo del piso falso debido a que como allí se encuentra cableado de datos y eléctrico con probabilidad de corto e inicio de incendio.

4. **Documentos físicos en los puestos de trabajo de la Entidad.**

Después de una jornada laboral, se hace observación de los puestos de trabajo de los funcionarios evidenciando que se están dejando documentos físicos encima de los puestos y no se están guardando en el mueble (credenza) asignado a cada cual.

Recomendaciones:

- ✓ Implementar y adoptar una política dentro del SIG respecto a puestos de trabajo despejados para documentación de papel y hacer énfasis en el resguardo dentro de la credenza asignada a cada funcionario.
- ✓ Sensibilizar, socializar y hacer monitoreo de la aplicación de la política de puestos de trabajo despejados por parte de funcionarios y contratistas.

5. Cableado estructurado :

Se realiza inspección física del cableado de datos y eléctrico en las instalaciones de la Defensoría y como resultado de la muestra se obtiene:

- Para pocos casos, se tienen pc´s (CPU y monitor) conectados a la corriente normal. Durante la visita los casos evidenciados se iban corrigiendo inmediatamente por la Oficina de sistemas, no obstante, durante el proceso de arreglo del cableado de cada puesto de trabajo se va a hacer un barrido general para atender este tema.
- Se observan tomas de corriente regulada y normal sin las tapas protectoras.

Recomendación:

- ✓ Realizar una revisión completa por toda la planta física de la entidad con el fin de validar el estado de las tomas de corriente y punto de red, y para los casos que amerite realizar la adquisición e instalación de las tapas protectoras.
- ✓ Sensibilizar y socializar al personal respecto al uso de la red de corriente normal y corriente regulada.

6. Seguridad para portátiles :

Se indaga acerca de los equipos portátiles asignados a funcionarios de la Entidad, a lo que fue informado por parte de la Oficina de sistemas que no se cuenta con un control que asegure el equipo contra los puestos de trabajo, es decir estos no cuentan con guaya de seguridad.

Recomendación:

- ✓ Validar la adquisición de guayas con clave o candado y asignarla a cada funcionario que tenga asignado un pc portátil, lo anterior con el fin de minimizar el riesgo de sustracción de equipos.

7. **Documentación :**

Respecto a documentación se menciona lo siguiente:

- La Oficina de Sistemas entrega a esta auditoría el documento denominado "centro de cómputo DADEP" el cual contiene los lineamientos de operación dentro del data center, no obstante este documento no se encuentra oficializado dentro del SIG de la Entidad.
- Dentro de los procedimientos, guías o instructivos del proceso de gestión de la información y la tecnología oficiales, no se contemplan las actividades relacionadas con el alistamiento de equipos para entregar a la Subdirección Administrativa, financiera y de Control Disciplinario para su correspondiente proceso de baja.
- De igual manera, dentro de los procedimientos no tienen definidas políticas referentes a la seguridad de los laptop de la Entidad.

Recomendación:

- ✓ Incluir dentro de la documentación del proceso de gestión de la información y la tecnología todos los aspectos y/o actividades que se estén realizando actualmente en referencia a seguridad física pero que no estén contemplados dentro del SIG, tales como los mencionados en las observaciones.

V. RIESGOS

Basado en los hallazgos expuestos en este informe, se presentan los siguientes riesgos:

- Acceso físico no autorizado a las instalaciones.
- Fuga, revelación y copia de información electrónica y/o física.
- Robo de equipos.
- Daño de equipos.
- Indisponibilidad de información y de los recursos tecnológicos.
- Suplantación.

VI. OTRAS OBSERVACIONES

A continuación se exponen temas, los cuales se consideran de carácter importante pero que no implican un riesgo para las operaciones, mas sin embargo son mencionadas para su conocimiento:

- El sensor que activa la iluminación dentro del centro de cómputo se encuentra en la frente de los racks de servidores y comunicaciones, esto quiere decir que si se realizan trabajos en la parte posterior y después del tiempo de inactividad el sensor apaga la luz evitando una correcta ejecución de las labores, adicionalmente se observa que el sensor está encendiendo la luz sin existir personal dentro del centro de cómputo, por lo anterior se requiere una calibración.
- También derivado de la visita al centro de cómputo, se informó al Jefe de la Oficina de Sistemas acerca de la fecha de última revisión registrada en la etiqueta del tanque de gas del FM200 el cual data de diciembre de 2014, lo que indicaría que estaría vencido, sin embargo el Jefe de la Oficina manifiesta que la carga y revisión se realizó como corresponde pero el proveedor se equivocó al etiquetar el tanque y para tal fin se iba a solicitar la corrección del tema.
- Basado en la inspección física del cableado en los puestos de trabajo, se observa que el cableado (UTP, ratón, teclado, corriente, etc) puede verse afectado principalmente por los pies de los funcionarios ya que estos están expuestos. Dentro de la auditoría se estableció que derivado de una visita de la ARL, se encuentra en curso un plan de acción para atender este tema por parte de la Oficina de Sistemas, el cual se espera finalizar el mes de Noviembre de 2015.
- Como se mencionó en la observación del data center, la oficina de sistemas no cuenta con una bodega para almacenamiento de equipos de cómputo y otros

componentes de la plataforma tecnológica, es por esto que se tienen almacenados equipos y en general cajas con elementos electrónicos dentro del data center; también se observaron equipos de cómputo apilados en una esquina contigua a los puestos de trabajo de la Oficina de sistemas.

- Se realiza inspección física de los extintores distribuidos a lo largo de las Oficinas de la Entidad encontrando lo siguiente:
  - Se encuentran extintores sin aviso informativo en la Oficina de comunicaciones, en la sala plazoleta y en el centro de impresión y copiado.
  - Se encuentran avisos de extintores sin dichos elementos en la entrada oriental y occidental cerca a los puestos de los guardas de seguridad. Únicamente se visualizan las camillas de primeros auxilios.

VII. CONCLUSION

El esquema de seguridad física y ambiental que opera actualmente en la Entidad, permite atender y minimizar los riesgos relacionados con la interrupción de las operaciones y del servicio que presta la plataforma tecnológica recientemente renovada, aportando a la seguridad de la información y garantizando el correcto funcionamiento de los equipos de cómputo. No obstante, es de carácter importante tener en cuenta los aspectos mencionados con el fin de robustecer el tema de seguridad aplicando buenas prácticas e implementado controles acordes a las necesidades y al nivel de exposición que tenga la Defensoría.

Cordial Saludo,

WILLIAM VALDERRAMA GUTIERREZ
Jefe Oficina de Control Interno

Copia: Oficina de Sistemas y Subdirección Administrativa, Financiera y de Control Disciplinario.
Fecha: Noviembre 30 de 2015
Proyectó: Diego Urazán Franco
Revisó: William Valderrama Gutiérrez
Aprobó: William Valderrama Gutiérrez
Código de archivo: 1301901