OFICINA DE CONTROL INTERNO

AUDITORIA PROCESO DE TELEMATICA

OCTUBRE 2014

Recibí
Oct-24-2014
10:35 AM

ERIKA HARJ.
24/10/2014
10:08

1. RESUMEN EJECUTIVO

1.1. OBJETIVO:

Determinar la conformidad del sistema de gestión de seguridad de la información en el Proceso Telemática del Fondo Rotatorio de la Policía.

1.2. ALCANCE:

Verificar la seguridad de la información y controles del 01 de abril de 2014 hasta el 31 de julio de 2014.

1.3. CRITERIOS:

Ley 555 de 2000 Ley 962 de 2005 Disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y Entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios público, Sistemas de comunicación personal, Resolución 26930 de 2000 Estándares para el funcionamiento Entidades certificadoras , Decreto 994 de 1999, Decreto 2150 de 1995 Sistemas de trasmisión electrónica datos para lograr la comunicación efectiva, Decreto 527 de 1999 Se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Decreto 1747 de 2000 Certificados y firmas digitales, Entidades certificadoras, Decreto 2693 de 2012 Lineamientos Generales de Gobierno en Línea, Modelo Estándar de Control Interno (MECI), NTCGP 1000: 2009, Acuerdo 012 de 2013 "Estatuto del Fondo Rotatorio de la Policía" Norma Técnica ISO 27001:2013, Instructivo para la gestión de la seguridad de base de datos" y de la legislación aplicable a la seguridad de la información.

2. FORTALEZAS DE CONTROL

Se cuenta con el DATA CENTER de la Entidad según criterio del Experto Técnico John Walter Mendez Manjarrez, cuenta con las condiciones óptimas para el desarrollo de las actividades de la Entidad, bajo las normas establecidas por seguridad informática, en un espacio adecuado el cual está capacitado para adaptaciones y regulaciones, sistema de refrigeración, alarma detectora contra incendios y corriente regulada a tiempo completo.

Comunicaciones unificadas a través del correo Microsoft Exchange el cual brinda a la Entidad nueva forma de comunicación interactiva a través de video cámara, teléfono, conferencia, transferencia de datos y archivos.

El Grupo de Telemática gestiono con oportunidad y eficiencia la adquisición de nuevos equipos de computación el cual está brindando a la Entidad seguridad en el apoyo de sistemas de información contribuyendo a mejorar los procesos de la Entidad.

a. Ubicación y protección de los equipos de cómputo.
b. Servicios de suministro de energía.
c. Seguridad del cableado estructurado.
d. Mantenimiento de equipos.
e. Retiro de activos.
f. Seguridad de equipos y activos fuera de las instalaciones.
g. Disposición segura o reutilización de equipos.
h. Política de escritorio limpio y pantalla segura.

Frente a la ubicación de los equipos fue presentada una sensibilización a través del correo interno de la Entidad dirigida hacia los usuarios acerca de las acciones que afectan la seguridad de la información.

Así mismo, se observó falencia en el cableado en los diferentes Grupos porque se ven cables y conexiones inseguras, en donde pueden afectarse los usuarios, activos y otras interrupciones ocasionando fallas en el servicio.

7. Al verificar los procedimientos operacionales y responsabilidades que establece la norma "*Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información*" se revisó el procedimiento PG.2.1.1 Atención Requerimientos Telemáticos, donde se observó que algunas actividades ya no se desarrollan el proceso tal como:

a. El administrador de la mesa de ayuda no está ingresando los datos del TAR ya que lo hace el mismo usuario.
b. El requerimiento en el sistema lo ingresa el usuario.
c. El Grupo de Telemática no consulta la base de datos, en donde se evidencie que después de varios TARES, se depura la información para dar solución definitiva.

8. Se revisó la disposición referente *"Proteger contra la perdida de datos"* a la fecha no se evidenció registros documentado de la restauración del backup de la información de la Entidad, y controles que determinen su efectividad.

   Así mismo, no existe un servidor fuera de la Entidad que salvaguarde y recupere la información perdida en el momento presentarse en caso de riesgos y catástrofes naturales.

9. Se analizó frente a la norma "*Prevenir el aprovechamiento de las vulnerabilidades técnicas*" teniendo en cuenta que el día 28 de julio de 2014 el Fondo Rotatorio de la Policía fue atacado cibernéticamente, según informe sin fecha de la firma Micrositios S.A.S, Outsourcing encargada de la página WEB, con nombre técnico

Sistema de Gestión dictado por ICONTEC a partir del 16 de junio a 5 de agosto de 2014, cumpliendo con noventa y seis (96) horas presencial, gracias a un cupo obsequiado por la Policía Nacional, sin embargo el mencionado funcionario presento la renuncia el día 01 de octubre de 2014 siendo el encargado de la seguridad de la información en la Entidad. Actualmente está función la desempeña la funcionaria Tecnóloga en Sistemas Angie Yamile Beltran Contreras, por lo tanto se concluye que continua la debilidad de capacitación.

5. LISTA DE HALLAZGOS DE LA AUDITORIA

HALLAZGOS	NORMA	RIESGO
1- Las políticas del Sistema de Información establecidas en Gobierno en Línea no están documentadas de acuerdo con los diferentes niveles de maduración como son: a. Seguridad de la información. b. Uso de dispositivos móviles y teletrabajo. c. Acceso a redes y a servicios de red. d. Ingresos de los usuarios e. Amenazas externas y ambientales f. Respaldo de información (backup) g. Seguridad en las comunicaciones h. 8. Proveedores de materiales y servicios	Decreto 2693 de 2012 Artículo 7. "Modelo de Gobierno en Linea" Sistemas de Gestión de la Seguridad de la Información ISO 27001.	Deficiencia en la protección y seguridad física, infiltración cibernética, perdida de la confidencialidad, de los recursos financieros, información de la Entidad, clientes y proveedores.
2- Los incidentes informáticos no son documentados, comunicados, ni generan espacios para la toma de decisiones y la solución del problema en temas prioritarios que dispone Gobierno en Línea, en donde se evidencie las medidas tomadas o alternativas de contingencias para mitigar la materialización de los riesgos.	Decreto 2693: Artículo 6. "*Temas prioritarios para avanzar en la masificación de Gobierno en línea*". Sistemas de Gestión de la Seguridad de la Información ISO 27001 numeral A.16.1 *"Gestión de Incidentes y mejoras en la seguridad de la Información"*	Al no reportarse y documentar las falencias del sistema, y no tomar acciones preventivas y correctivas se puede incurrir nuevamente en el mismo incidente.

CONCLUSIONES:

1. El Grupo de Telemática cuenta con un proyecto desde 30 de abril de 2014 "*Manual del Sistema de Gestión de Seguridad de la Información para Fondo Rotatorio de la Policía*" donde están incluidas las políticas, directrices para la toma de decisiones y el cumplimiento de la norma ISO 27001:2013. A la fecha no ha sido presentado para la revisión de la Oficina Asesora de Planeación y la aprobación por el Director.

d) las instalaciones están debidamente protegidas con canaletas para interiores o tubos metálicos para instalaciones externas.

7- Los equipos que se encuentran en funcionamiento y a servicio de la Entidad deben tener un control de la descripción y frecuencia del mantenimiento correctivo y preventivo de forma individual.

Contador Público **HAMILTON STEVE VIRGÜEZ RAMIREZ**
Profesional Oficina de control interno

Administradora de Empresas **CAROL LILIANA REINA DIAZ**
Auditora Oficina de Control Interno

Abogada **ELVIA CONSTANZA GARCIA ORTEGA**
Jefe Oficina de Control Interno (E)

"SERVICIO CON PROBIDAD"