

| | | |
|--------------------------|--|---|
| Código: F92 | INFORME DE AUDITORIA DE SISTEMAS DE GESTIÓN |  |
| Versión: 2 | | |
| Fecha: 12/03/2019 | | |
| Página 1 de 2 | | |

| | | | |
|---|---|--------------------------------|---|
| FECHA DEL INFORME: | 30/08/2019 | PROCESO AUDITADO: | Ingreso Administración de personal |
| LIDER DEL PROCESO: | Coordinadora Grupo de Talento Humano | AUDITADOS: | Miriam Cardona Giraldo – Coordinadora Grupo de Talento Humano Johana Niño Acosta – Analista Claudia Stella Cortés – Coordinadora de Riesgos No Financieros |
| AUDITOR LÍDER: | Adriana Aranguren | EQUIPO AUDITOR: | Adriana Aranguren |
| LUGAR Y FECHA DE REALIZACIÓN DE AUDITORÍA: | Sede Principal Grupo de Talento Humano Piso 8 23/08/2019 | CRITERIOS DE AUDITORÍA: | Norma Técnica ISO 27001:2013 Lineamientos de MinTIC del Modelo de Seguridad y Privacidad de la Información, Política de Gobierno Digital y Política de Seguridad Digital. Documentación del Sistema de Gestión de Seguridad de la Información. Planes de mejoramiento. Normatividad aplicable. |

1. OBJETIVO

Evaluar el cumplimiento o la conformidad del Sistema de Gestión de Seguridad de la Información y Modelo de Seguridad y Privacidad de la Información, de acuerdo con los requisitos de las normas técnicas vigentes aplicables, normativos y de la Entidad; en los procesos de Ingreso y Administración de personal y sus procedimientos, identificando oportunidades de mejora.

2. ALCANCE

Se auditó la gestión general del proceso teniendo en cuenta las actividades realizadas del año 2018 hasta la fecha, con base en el ciclo PHVA y el cumplimiento de normas y lineamientos transversales del Sistema de Gestión de Seguridad de la Información, en lo aplicable al proceso.

3. FORTALEZAS

Se destaca la buena disposición para la atención de la auditoría por parte de las auditadas, la disponibilidad de la información y el conocimiento acerca de las políticas de seguridad de la información.

4. RESULTADOS

| CRITERIO DE AUDITORIA | NO CONFORMIDAD | OPORTUNIDAD DE MEJORA |
|--|-----------------------|--|
| Norma ISO 27001:2013 Anexo A Dominio A.8 Gestión de activos A.8.1. Responsabilidad sobre los activos A.8.2. Clasificación de la información Ley 1712 de 2014 Decreto 103 de 2015 | | Se debe revisar y ajustar el inventario de activos de información, porque para el activo “Historias laborales” se evidencia en auditoría su almacenamiento en medio físico, pero en el inventario aparece como “digital”; dado que según se informa se está iniciando la digitalización de las mismas. Igualmente, para el activo “planta de personal” no es claro en la descripción |

| | | |
|--------------------------|--|---|
| Código: F92 | INFORME DE AUDITORIA DE SISTEMAS DE GESTIÓN |  |
| Versión: 2 | | |
| Fecha: 12/03/2019 | | |
| Página 2 de 2 | | |

| | | |
|---|--|--|
| Decreto 1081 de 2015 Resolución 3564 de 2015 | | qué tipo de información personal contiene; la cual se considera “clasificada”. |
| Norma ISO 27001:2013 Anexo A A.15. Relación con los proveedores A.15.1.1. Políticas de seguridad de la información con proveedores A.1.5.1.2. Requisitos de seguridad en contratos con terceros | No se cuenta con un acuerdo de intercambio de información con el proveedor de estudios de seguridad del personal que ingresa a la entidad. Esto incumple con el control A.13.2.2 Acuerdos de Intercambio de información, del Anexo A de la Norma ISO 27001:2013. | |
| Norma ISO 27001:2013 7.5.3. Control de la información documentada | Se mantiene la no conformidad: "Se evidencia uso de corrector en la planilla de reporte de horas extras para el día 16 de Octubre de 2017; incumpliendo de esta forma con lo establecido en la Norma ISO 27001:2013 en el numeral 7.5.3 (B) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad)." | |

5. CONCLUSIONES

Se han logrado el objetivo y alcance de la auditoría y se puede concluir, con base en la muestra auditada, que el proceso presenta una “no conformidad” con respecto a los requisitos de la norma técnica ISO 27001:2013 y demás criterios aplicados. Además, se mantiene abierta una no conformidad proveniente de la auditoría interna anterior; relacionada con el control de la información documentada. (Ver sección 4. Para observaciones relacionadas y recomendaciones para el plan de mejoramiento, consultar F86 - Seguimiento de acciones correctivas, documento adjunto). Las no conformidades deben ser corregidas y analizadas para definir e implementar acciones correctivas, de acuerdo con el procedimiento de la entidad. Así mismo, se detectó en la auditoría una oportunidad de mejora, la cual se recomienda analizar, con el fin de definir e implementar acciones que permitan evitar no conformidades en el futuro.

Como parte del seguimiento del plan de mejoramiento proveniente de los resultados de la anterior auditoría interna de seguridad de la información, también queda abierta la no conformidad referente a la seguridad en las puertas de acceso a los pisos; la cual fue inicialmente detectada en la auditoría a los procesos de Talento Humano; pero ha sido reasignada en el ejercicio de la presente auditoría al proceso de Administración de Activos Fijos; de forma tal que se tomen medidas de control de seguridad física, que eliminen la no conformidad en toda la entidad. Se cerraron las 7 no conformidades restantes, aunque se registraron observaciones (Ver F86, documento adjunto).

6. OBJECIONES DEL AUDITADO NO RESUELTAS

No aplica.