COMUNICACIÓN INTERNA

20201100013513

Radicado: **20201100013513** de 04-05-2020

Bogotá D.C, lunes 04 de mayo de 2020

PARA: Martha Lucia Cardona Visbal

DE: Oficina de Control Interno

ASUNTO: Entrega Informe Auditoria Interna Proceso Gestión de Tecnología

Respetada Doctora:

La Oficina de Control Interno en el rol de evaluación y seguimiento, hace entrega del Informe de Auditoría Interna al Proceso Gestión de Tecnologías, resaltando que dicho informe se socializó en reunión de cierre el pasado 30 de abril, donde se aceptaron de conformidad los 4 hallazgos identificados.

Respecto a las conclusiones de la auditoría, se recomienda realizar la divulgación del informe y elaborar el plan de mejoramiento, con el acompañamiento de la Oficina Asesora de Planeación de acuerdo con los procedimientos vigentes. Cabe señalar que la Oficina de Control Interno realizará la respectiva asesoría metodológica sobre acciones correctivas, preventivas y de mejora.

De conformidad con lo establecido en la Ley 1712 de 2014, Arts. 9, lit d) y 11, lit e), el informe en mención será publicado en la página web institucional, sección transparencia – Informes de Control Interno.

Cordialmente,

Angélica Hernández Rodríguez
Jefe Oficina Control Interno.

c/c. Adriana Padilla Leal – Directora General FUGA
Margarita Díaz - Subdirectora para la Gestión del Centro de Bogotá
César Parra Ortega – Subdirector Artístico y Cultural
John Fredy Silva– Jefe Oficina Asesora Jurídica
Luis Fernando Mejía - Jefe Oficina Asesora de Planeación
*Comité Institucional de Coordinación de Control Interno

Edwin Díaz – Proceso Gestión de Tecnologías
Ernesto Ojeda – Proceso Gestión de Tecnologías

Proyecto: María Janneth Romero Martínez – Contratista OCI
Anexo (16) folios – Informe y Anexo Instrumento Evaluación MSPI

FECHA DE EMISIÓN DEL INFORME	Día:	30	Mes:	04	Año:	2020

Proceso:	Gestión de Tecnologías de la Información
Líder de Proceso / Responsable Operativo Auditado:	Martha Lucia Cardona Visbal – Subdirectora de Gestión Corporativa Edwin Díaz – Profesional Contratista TI
Objetivo de la Auditoría:	Verificar el diseño y ejecución de los controles que garantizan el cumplimiento de los requisitos internos y externos asociados a la gestión del Proceso Gestión de Tecnología, así como la implementación de controles que permitan el cumplimiento de la misionalidad de la Entidad * Identificar oportunidades de mejora.
Alcance de la Auditoría:	Revisión realizada al periodo comprendido del 01-01-2019 al 31/01/2020 / Proceso Gestión de Tecnología
Criterios de la Auditoría:	• Modelo de Seguridad y Privacidad de MINTIC • Norma técnica colombiana NTC - ISO/IEC 27001 • Guía para la administración del riesgo y el diseño de controles en entidades públicas. Función Pública - octubre de 2.018 • MIPG • Documentos SIG vinculados al proceso

Reunión de Apertura						Ejecución de la Auditoría				Reunión de Cierre					
Día	05	Mes	03	Año	2020	Desde	05/03/2020	Hasta	27/04/202	Día	30	Mes	04	Año	2020

Jefe Oficina de Control Interno	Equipo Auditor
ANGELICA HERNÁNDEZ RODRÍGUEZ	Auditor Líder: MARÍA JANNETH ROMERO MARTÍNEZ

RESUMEN EJECUTIVO

DESARROLLO DE ACTIVIDADES

La Oficina de Control Interno, de conformidad con el Plan Anual de Auditoras Internas versión 0, aprobado en sesión del Comité Institucional de Coordinación de Control Interno (CICCI) - Comité Directivo de fecha 30 de enero de 2020; realizó la reunión de apertura de Auditoria al Proceso *Gestión de Tecnologías* el 05 de marzo de 2020, donde se presentó el Plan de Auditoria, el cual fue aceptado en su totalidad por el equipo auditado. El

cronograma se desarrolló con normalidad entre el 17 de febrero y 30 de abril de 2020, como se relaciona a continuación:

ITEM	ACTIVIDAD DE AUDITORIA	AUDITOR RESPONSABLE	CRONOGRAMA
			Febrero / Marzo / Abril / na
1	SOLICITUD DE INFORMACIÓN INICIAL	María Janneth Romero M	
2	VERIFICACIÓN DE LA INFORMACION RECIBIDA	María Janneth Romero M Raul Ernesto López	
3	REUNIÓN DE APERTURA	Angélica Hernández Rodríguez	
4	SOLICITUD DE INFORMACION TENIENDO EN CUENTA EL OBJETO Y ALCANCE DEFINIDOS	María Janneth Romero M	
5	DETERMINACIÓN DE LA MUESTRA DE AUDITORIA	María Janneth Romero M	
6	DISEÑO DE PAPELES DE TRABAJO y PRUEBAS DE AUDITORIA	María Janneth Romero M	
7	APLICACIÓN DE PRUEBAS DE AUDITORIA (Entrevistas, trabajo in situ, revisión documental)	María Janneth Romero M	
8	ANALISIS Y EVALUACION DE DATOS	María Janneth Romero M Raul Ernesto López	
9	ELABORAR INFORME PRELIMINAR	María Janneth Romero M	
10	REUNION DE CIERRE - PRESENTACIÓN DE RESULTADOS (INFORME PRELIMINAR)	Angélica Hernández Rodríguez	
11	ACTIVIDADES DE REVISIÓN	María Janneth Romero M	
12	PRESENTACIÓN DEL INFORME DEFINITIVO	María Janneth Romero M	

En la reunión de cierre realizada el 30 de abril se presentó el informe preliminar y el equipo auditado en cabeza de la líder de proceso, manifestaron que no se pronunciarán sobre las conformidades de los Hallazgos puntualizados en el informe. Después finalizada la reunión se remite a través de correo electrónico el acta correspondiente al desarrollo de la misma y el formato de evaluación de auditoria

FORTALEZAS

- Disposición y cordialidad de los delegados para atender las entrevistas de auditoría
- El acceso a la información y la oportuna entrega de las evidencias requeridas para la ejecución del ejercicio de auditoría
- El conocimiento de la entidad y la experticia respecto a los temas evaluados, demostrada por el equipo auditado en el desarrollo de las entrevistas y aplicación de las listas de verificación.
- Se cumplió de manera oportuna la entrega de información requerida para el desarrollo de la auditoria.

OPORTUNIDADES DE MEJORA Y RECOMENDACIONES

De acuerdo a las técnicas de auditoria aplicadas en el desarrollo del presente ejercicio, cuyos procedimientos se fundamentaron en la consulta, observación, inspección, y confirmación; se presentan a continuación los aspectos más relevantes evidenciados por el equipo auditor, de conformidad con los criterios evaluados, definidos en la etapa de planeación de la auditoría:

1. Evaluación de la Ejecución de los planes vinculados al Proceso de Gestión de Tecnología en el periodo auditado (2019 y corrido 2020).

1.1. Plan Estratégico de Tecnologías de Información y Comunicaciones – PETIC

De conformidad con los controles evidenciados en el PETIC establecidos para las dos vigencias, se observa que no se ha dado cumplimiento o ha sido parcial en los siguientes aspectos:

7. POLÍTICAS INFORMÁTICAS INTERNAS Y DE SEGURIDAD

- Cumplimiento parcial de lo indicado en el literal c. Asistencia y Capacitación: En el documento se establece: "…*programas <u>permanentes</u> de inducción, capacitación y entrenamiento de uso de tecnologías de información y comunicaciones*" (Subrayado fuera de texto); no obstante, de acuerdo a lo indicado en la aplicación de la lista de verificación el día 06/04/2020, en el 2019 estas se llevaron a cabo conforme necesidades particulares (ingreso y a solicitud de los interesados). Para la vigencia 2020 si bien se incluyen dos actividades vinculadas a TIC en el Plan de Capacitación Institucional (PIC), estas están orientadas a promover herramientas informáticas y gobierno en línea.
- No se realizó la divulgación periódica a través de intranet y mensajes a correos electrónicos a cada uno de los funcionarios, de las políticas de seguridad conforme se establece en el literal i. De acuerdo a lo indicado en la aplicación de la lista de verificación, ésta se lleva a cabo cuando se presta soporte in situ.
- No se lleva a cabo la socialización de los avances y documentación de los proyectos en la intranet. (literal j. Documentación de proyectos)

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

- No se llevó a cabo la entrega trimestral a Gestión Documental de las copias de seguridad de los sistemas de información en medio magnético ((literal b. Copias de seguridad de los sistemas de información PETIC 2019).
- No se evidencia la divulgación periódica de las políticas de seguridad durante la vigencia (PETIC 2019)

17. PLANES DE CONTINGENCIA 2019 (NUMERAL 9 PETIC 2020)

- No se realizó la entrega de las copias de respaldo de la información mes a mes a Gestión Documental para su almacenamiento fuera de la entidad. (Literal b. A nivel de TIC), conforme lo indicado por los responsables operativos, esta gestión se lleva a cabo en el servidor NAS pero no se tiene contrato para el almacenamiento del respaldo fuera de la entidad.

a. Avance Ejecución de las estrategias del Plan (2019 y 2020):

A continuación, se presenta lo informado por los responsables operativos respecto a la implementación de las estrategias establecidas en el plan durante el periodo auditado:

ESTRATEGÍA	GESTIÓN
Adoptar el uso de tecnologías de información y comunicaciones, por parte de los funcionarios, contratistas, usuarios en la Entidad, a su vez generando espacios de permitan las mejores prácticas y automatización de procesos	2019: VPN y teletrabajo con relación a la prueba piloto (Financiera - Presupuesto) 2020: Si bien no se encuentra dentro del periodo auditado, en el mes de marzo se aplicó a toda la entidad en el periodo de contingencia COVID 19 Publicamos acceso ORFEO. Estrategia comunicada a nivel directivo.
Desarrollar y adquirir habilidades y competencias organizacionales para el uso de tecnologías de información y comunicaciones.	2019 y 2020: Contrato para poder tener las herramientas G y Suite con Gsuite (El contrato es con Ito Software SAS para el 2019) el contrato ayuda para usar las herramientas de Gmail (correo, calendario, drive, formularios, entre otras). Su divulgación se hace in situ conforme demanda
Establecer políticas y procedimientos de uso e implementación de las tecnologías de información y comunicaciones (TIC) en la Entidad.	Adaptar las políticas que vienen desde MINTIC y la Alta Consejería TIC para implementarlas al contexto tecnológico de la Fundación
Suministrar, dotar y mantener a la entidad con herramientas de cómputo y comunicaciones de última tecnología.	Esfuerzo que se hace todos los años solicitando asignación de recursos para atender las necesidades tecnologías de la entidad a través del PAA. En términos de mantenimiento se tiene un contrato que respalda esta labor.
Garantizar la disponibilidad, confiabilidad en los sistemas de información y comunicaciones.	Lo que se hace básicamente es con el servicio de conectividad con los enlaces para poder comunicar las sedes con el interior y el exterior (a través de fibra óptica) Proveedor: Media Commerce
Aplicar tecnologías de información y comunicaciones que promuevan la democratización de la información, la interoperabilidad y el intercambio de información.	Democratización: Accesible para todo el público Se hace a través de Datos Abiertos y la publicación en la página web Link de transparencia de la información asociada a los activos de información
Implementar un gestor documental que permita la eficiencia en el trámite documental al interior de la entidad y así mismo minimice al máximo el uso de papel en la FGAA.	ORFEO
Promover la implementación de software libre al interior de la entidad para ofrecer mejores prácticas y procedimientos	KOHA y ORFEO

Fuente: Lista de Verificación Planes 06/04/2020

Conforme lo expuesto por el proceso es importante señalar que esta gestión no se encuentra documentada, sino que corresponde al conocimiento y experticia de los responsables operativos en la implementación de lo señalado anteriormente.

b. Ejecución de los Proyectos a Implementar de acuerdo a lo definido en el Plan (2019)

El Plan Estratégico de Tecnologías de la Información y Comunicaciones PETIC publicado en el 2019, corresponde al plan formulado para los años 2016 a 2020, e incluye los siguientes proyectos o actividades a desarrollar en ese periodo:

- PY01 Análisis, Diseño e Implementación de Koha:

- PY02: Actualización e Implementación de procesos de la Dirección de TIC
- PY03: Diseño del Subsistema de Gestión de la Seguridad Informática
- PY04: Renovación de Infraestructura Tecnológica:
- PY05: Aplicación Clubes y Talleres:
- PY06: Traslado de UPS casa principal:
- PY07: Software ERP Sistema Financiero Contable FUGA:
- PY08: Desarrollo para Jurídica-Financiera-Planeación:
- PY09: Adecuación Cableado Estructurado Torre Casa Principal:
- PY10: Adecuación Interconexión de sedes con una única salida de internet:
- PY11: Segmentación de Servicio WIFII y Cambio de Contraseñas:

De los anteriores proyectos se observa que siete (7) tenían plazo estimado de terminación en el 2018 (PY01, PY04, PY05, PY06, PY09, PY10 Y PY11), plazos que fueron cumplidos de acuerdo a lo informado por los responsables operativos del proceso, en la aplicación de la lista de verificación del 06/04/2020

En el 2019 se tenía proyectado desarrollar el PY08 (*Desarrollo para Jurídica-Financiera-Planeación*), proyecto que no se llevó a cabo por cuanto no se contó con los recursos para su desarrollo e implementación. De acuerdo a lo indicado por los responsables operativos del proceso, "*se inició con una línea base de requerimientos y estos fueron desbordados por lo cual no se logró el desarrollo de lo previsto*"

Respecto a la ejecución de los proyectos estimados para el 2020 (PY02 y PY03) se evidencia que fueron incluidos en el plan presentado en el 2020, cuyo alcance comprende el cuatrienio 2020 a 2024, ajustando también las fechas estimadas de terminación y los nombres de los mismos; aunque se mantienen conforme se formularon en el cuatrienio anterior, la descripción del proyecto, entregables esperados, indicadores básicos, riesgos de no hacerlo y demás información del mismo.

Por último, se observa la formulación de un proyecto con fecha estimada de terminación en el 2021 (*PYPY07: Software ERP Sistema Financiero Contable FUGA*), el cual no se encuentra incluido en el plan del cuatrienio 2020 – 2024, y sobre el particular se indica que se gestionó a través del Contrato con Soporte Lógico.

Sobre este particular y de acuerdo a la verificación realizada por la OCI se observa que en la vigencia 2019 se suscribieron dos contratos de soporte y acompañamiento técnico, así:

- FUGA-77-2019: Contratista: IDEASOFT LIMITADA: Objeto: "*Prestar con plena autonomía técnica y administrativa el servicio de soporte y acompañamiento técnico al aplicativo Visual Summer con el que cuenta la Fundación Gilberto Álzate Avendaño*". Sistema para los Módulos de Contabilidad y Tesorería
- FUGA-100-2019: Contratista SOPORTE LÓGICO LTDA. Objeto: "*Prestación de servicio de arrendamiento, soporte, actualización y mantenimiento al sistema de información HUMANO y CONTAR*". Módulos de Gestión Humana (nomina, gestión humana y seguridad y salud en el trabajo) a través de HUMANO e Inventario y Almacén a través de CONTAR

Conforme lo anterior y teniendo en cuenta que uno de los entregables esperados del proyecto era el de "*Integrar todas las dependencias de la entidad al aplicativo y velar por su funcionamiento y mantenimiento*" se observa que de manera general se ejecutó el proyecto; no obstante, es importante señalar que, si bien el sistema Visual Summer integra la información financiera generada desde los sistemas HUMANO y CONTAR, esta se lleva a cabo a través de interfaz, por lo que se recomienda definir de manera precisa el alcance y demás componentes de los proyectos de tal manera que no se presenten ambigüedades en el momento de soportar su ejecución.

Por último, es importante mencionar que al corte de marzo de 2020 se observa la suscripción del contrato FUGA-26-2020 con IDEASOFT LIMITADA cuyo objeto es: "*Prestar el servicio de soporte y acompañamiento técnico al aplicativo "Visual Summer" con el que cuenta la Fundación Gilberto Alzate Avendaño*". No obstante no se evidencia contrato para dar continuidad al soporte, actualización y mantenimiento HUMANO y CONTAR

c. Avance Ejecución de los Proyectos a Implementar de acuerdo a lo definido en el Plan (2020)

El Plan Estratégico de Tecnologías de la Información y Comunicaciones PETIC publicado en el 2020, corresponde al plan formulado para los años 2020 a 2024, e incluye los siguientes proyectos o actividades a desarrollar en ese periodo:

- PY01 Análisis, Diseño e Implementación de Micrositio SIG:
- PY02: Actualización e Implementación de procesos de la Dirección de TIC Gobierno Digital
- PY03: Implementación de Documentos asociados a Seguridad Digital
- PY04: Compra de Elementos Tecnológicos – Sotware y Hardware:
- PY05: Tratamiento de datos personales:
- PY06: Contrato de Servicios de Interconexión y Servicio de Internet:

Teniendo en cuenta las fechas estimadas de finalización de estos proyectos, se observa que cuatro (4) de ellos están formulados para el 2020; sobre el particular es importante señalar que el proyecto *PY01 Análisis, Diseño e Implementación de Micrositio SIG,* si bien tiene fecha de vencimiento en el mes de marzo, el proceso señala que no se ha ejecutado por cuanto su desarrollo estaba bajo la responsabilidad del Web Master, cuyo contrato inicio el 25/02/2020 (FUGA-47-2020); de la verificación realizada a las obligaciones contractuales establecidas no se observa cómo se vinculan estas al objetivo específico del proyecto: "*Proveer un gestor de WEB que permita tener un catálogo en línea y centralizada la información correspondiente al SIG*"

1.2. Plan de Tratamiento de Riesgos de Seguridad y Privacidad en la Información:

Ejecución Plan (2019):

El plan identifica 5 riesgos de seguridad digital:

Riesgos Seguridad de la Información	Vulnerabilidades	Valoración Inherente	Actividades de Tratamiento	MONITOREO PROCESO GESTIÓN DE TECNOLOGIAS

ACCESO NO AUTORIZADO A LA INFORMACIÓN	Acceso a los recursos e información del Sistema	**Riesgo Alto**	Definir políticas y procedimientos e implementar mecanismos de seguridad que permitan tener en cuenta tanto para funcionarios como contratistas, establecer sus responsabilidades, tomar conciencia, usar de manera aceptable y con acceso seguro a los activos de información de la entidad.	Se actualizaron procedimientos en el 2019, se vincularon adiciones para mejorar el procedimiento e implementar temas que no se tenían parametrizadas. Ejemplo copias de seguridad en los procedimientos
ATAQUES EXTERNOS O INTERNOS	Desconocimiento de licenciamiento de software	**Riesgo Alto**	Conocer y ejercer un adecuado control del licenciamiento de software adquirido, acuerdos de licenciamiento y uso legal, suministrando una política para mantener las condiciones apropiadas.	Formatos de Hojas de Vida (Derechos de autor) Validación del licenciamiento permitido Documento dentro de los procedimientos que incluye el tema de activos de información
DAÑO DE LA INFORMACIÓN	Desconocimiento de normativa de seguridad	**Riesgo Alto**	Diseñar y poner en marcha un programa de sensibilización que permita la toma de conciencia tanto de funcionarios como contratistas, establecer sus responsabilidades, usar de manera aceptable y con acceso seguro los activos de información de la entidad.	No se llevó a cabo
DENEGACIÓN DE SERVICIO	Falta de disponibilidad de los servicios	**Riesgo Alto**	Asegurar que los servicios TI estén disponibles y funcionen correctamente, mediante la adecuación de mejoras en la infraestructura y servicios TI con el objetivo de mantener los niveles de disponibilidad.	Se llevó a cabo a través del contrato de MEDIA COMMERCE
CONFIGURACIÓN DE SEGURIDAD INCORRECTA	Falta de personal capacitado	**Riesgo Alto**	Contar con personal capacitado, con deberes y responsabilidades claras sobre la seguridad de la información para brindar apoyo a los procesos de gestión de la información de la entidad.	Los contratos de prestación de servicios.

Sobre el particular se observó:

Riesgo: ATAQUES EXTERNOS O INTERNOS: Si bien el proceso indica que se implementaron los formatos de hojas de vida, es importante precisar que conforme a los resultados del seguimiento realizado por la OCI al cumplimiento de las normas en materia de Derechos de Autor software vigencia 2019, se evidencio:

"Teniendo en cuenta las debilidades en el registro de la información en el formato GTI-FT-90 Hoja de Vida Equipos BASE DE DATOS 2019, relacionada específicamente con el número que identifica los equipos y su correlación con el usuario responsable, la dependencia y la identificación del procesador del equipo; se recomienda nuevamente registrar de manera integral, toda la información establecida en el formato Hoja de Vida Dispositivos Tecnológicos (GTI-FT-

90) Versión 5, de tal manera que ésta permita realizar un adecuado control, monitoreo y seguimiento a los recursos tecnológicos de la entidad (Software y Hardware).”

Respecto a la formulación realizada en el 2019 de los Riesgos y su tratamiento, se llevó a cabo la verificación de la Política de Administración de Riesgo de la entidad (CEM-PO-01) versión 2 con última fecha de actualización 30/04/2019; específicamente en los lineamientos relacionados con riesgos de Seguridad Digital de conformidad con el *Modelo de Gestión de Riesgos de Seguridad Digital (MGRS)* indicados Anexo 4 *Lineamientos para la Gestión de Riesgos de Seguridad Digital en entidades Púbicas* de MINTIC, Viceministerio de Economía Digital y Dirección de Gobierno Digital; donde se evidencia:

- No se identifica de manera clara el alcance para aplicar la gestión de riesgos de seguridad digital (Numeral 4.1.2)
- No se identifica quien es el responsable de Seguridad Digital en la entidad por tanto no se indican de manera específica las responsabilidades designadas a este. (4.1.4)
- Respecto a la identificación de activos de seguridad digital (4.1.6), si bien se observan publicados en el ítem *Registro de Activos de Información* (link de Transparencia de la página web) los Formatos *Gestión de Activos de Información (Software, hardware y servicios – Documentos y Archivos - Biblioteca – Obras de Arte)*, los cuales cumplen con las condiciones de: identificar los dueños de los activos, clasificación de activos, clasificación de información y determinación de la criticidad del activo; no se identifican los procesos a los que corresponden los activos y si existen infraestructuras criticas cibernéticas. De igual manera se observa que sólo se encuentra el listado de activos: Biblioteca Especializada en Historia Política de Colombia, Gestión Documental y Atención al Ciudadano y la Subdirección para la Gestión del Centro
- El Mapa de Riesgos de la entidad, no integra en los riesgos del Proceso Gestión de Tecnologías, todos los identificados en el plan de tratamiento de riesgos y todos los aspectos establecidos en la guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas. (Activo, tipo, amenazas e indicador).
- En el documento Plan de Tratamiento de Riesgo de Seguridad de la Información publicado por el Proceso Gestión de Tecnología, no se observa la identificación de las amenazas. (4.1.7)

Avance Ejecución Plan (2020):

El plan tiene como objetivo general: “*Crear un documento de lineamientos para el tratamiento de los Riesgos de la seguridad de la información*.”

Las metas y actividades previstas en el plan son:

META	ACTIVIDAD
1 documento que indique las acciones que debe realizar el personal correspondiente para proteger el Acceso no autorizado de los recursos e información	Generar una guía/procedimiento que permita controlar el acceso no autorizado a la información con el fin de que el personal pueda implementar buenas practicas
1 documento que contenga la relación de los activos de información a nivel de hardware y/o software con el fin de identificar los elementos que requieren protección o atención específica	Generar un inventario actualizado con relación a los activos a nivel de software y hardware que posee la entidad

1 documento que tenga la formulación del plan de comunicaciones con relación a seguridad de la información en la entidad para que pueda ser aplicado en el ámbito de la próxima vigencia	Formular un programa de sensibilización que permita la toma de conciencia y una divulgación adecuado de acuerdo al criterio técnico expresado
1 documento que contenga la relación de los activos críticos de la infraestructura TIC de la entidad que pueda ser vulnerable a un ataque informático	Genera un inventario actualizado de los activos críticos de la entidad

Fuente: Plan de Tratamiento de Seguridad de la Información vigencia 2020

Si bien estas actividades están programadas para ejecutarse entre febrero y diciembre de la vigencia, se precisa que no se identifica de manera clara los riesgos asociados al proceso y no es posible relacionar las actividades sobre las fases de tratamiento de riesgo.

Respecto al avance en la ejecución de las actividades previstas, el proceso indica que este documento está en proceso de ajustes y se definirá un nuevo plan para la vigencia 2020

1.3. Plan de Seguridad y Privacidad de la Información (PSPI)

a. Ejecución Plan vigencia 2019:

Fase Diagnóstico:

META	OBSERVACION OCI
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Se llevó a cabo a través del ejercicio de autoevaluación realizado por el proceso, a través del Instrumento Evaluación MSPI el cual fue presentado en la sesión del Comité Directivo de fecha 12/12/2019
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	
Determinar el nivel de madurez de los controles de seguridad de la información.	
Identificar el avance de la implementación del ciclo de operación al interior de la entidad.	

Fase Planificación:

META	OBSERVACION OCI
Política de Seguridad y Privacidad de la Información	Publicación Intranet (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)
Procedimientos de seguridad de la información.	Publicación Intranet (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)
Roles y responsabilidades de seguridad y privacidad de la información.	Los roles definidos son generales y no se establecen responsabilidades especificas
Inventario de activos de información.	Publicación Web: https://www.fuga.gov.co/transparencia/activos-informacion
Integración del MSPI con el Sistema de Gestión documental	Conforme lo indicado por el proceso se ejecutó a través de la gestión realizada con ORFEO
Identificación, Valoración y tratamiento de riesgo.	Se presentan debilidades, señaladas en el ítem anterior.
Plan de Comunicaciones	No se evidencia

Fase Implementación:

META	OBSERVACION OCI
Planificación y Control Operacional	De lo observado se evidencia que las metas identificadas se encuentran aún en construcción y dependen del resultado de la evaluación de las fases de diagnóstico y planificación que se está llevando a cabo
Implementación del plan de tratamiento de riesgos.	
Indicadores De Gestión.	

Fase de Evaluación de Desempeño:

META	OBSERVACION OCI
Plan de revisión y seguimiento, a la implementación del MSPI.	No se ejecuta en la vigencia planteada
Plan de Ejecución de Auditorias	

Fase de Mejora Continua:

META	OBSERVACION OCI
Plan de mejora continua	No se ejecuta en la vigencia planteada.

La gestión relacionada con estas actividades se detalla de manera específica en el desarrollo del numeral *3. Verificación del nivel de madurez de la implementación del Modelo de Seguridad y Privacidad de la Información*, del presente informe

Avance Ejecución Plan (2020):

El plan tiene como objetivo general: "*Crear un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para la Fundación Gilberto Alzate Avendaño*."

Las actividades previstas en el plan, contemplan las siguientes características:

META	ACTIVIDAD
1 documento que como mínimo debe contener la fase de planificación	En esta fase se pretende identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información
1 documento que como mínimo debe contener la fase de implementación	Esta fase le permitirá a la Entidad llevar a cabo la implementación de la planificación realizada en la fase anterior del MSPI
1 documento que como mínimo debe contener acciones orientadas a la fase de evaluación y desempeño	El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas
1 documento que como mínimo debe contener acciones orientadas a la fase de mejora continua	En esta fase la Entidad debe consolidad los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunidad para mitigar las debilidades identificadas.

Fuente: Plan de Seguridad y Privacidad de la Información (PSPI) vigencia 2020

Respecto al avance en la ejecución de las actividades previstas entre los meses de febrero y diciembre, el proceso en la aplicación de la lista de verificación de fecha 06/04/2020 indica que este documento está en proceso de ajuste

1.4. Plan de mantenimiento de servicios tecnológicos

El cronograma identifica 13 actividades cumplidas conforme lo observado en los soportes cargados en el servidor de la entidad en las rutas:

- \\192.168.0.34\plan operativo integral\OFICINA ASESORA DE PLANEACIÓN\Plan de Accion por Dependencia\Plan de acción por Dep 2019\Evidencias\Subdirección de Gestión Corporativa\TIC\CRONOGRAMA DE MTTO TIC

- \\192.168.0.34\plan operativo integral\OFICINA ASESORA DE PLANEACIÓN\Plan de Accion por Dependencia\Plan de acción por Dep 2019\Evidencias\Subdirección de Gestión Corporativa\TIC\Sgsi

No se evidencia el Plan establecido para la vigencia 2020 publicado en la página web de la entidad (https://www.fuga.gov.co/transparencia/plan-mantenimiento-servicios-tecnologicos)

2. Revisión documental de las guías, procedimientos, políticas y demás documentos SIG, vinculados al Proceso de Gestión de Tecnología.

De la revisión efectuada por el equipo auditor a los documentos publicados por el proceso tanto en la página web como en la intranet de la entidad, se observaron oportunidades de mejora relacionadas con los siguientes aspectos:

2.1. Plan de Mantenimiento Infraestructura Tecnológica (GTI-PL-01) Versión 1, publicado en la página web ((https://www.fuga.gov.co/planes-estrategicos-sectoriales-e-institucionales):
- No se publica el *Anexo 1. Cronograma de mantenimiento Infraestructura física* (Vigencia 2019)
- No se evidencia la publicación del plan para la vigencia 2020

2.2. Plan de Seguridad y Privacidad de la Información 2019 Versión 1, publicado en la página web ((https://www.fuga.gov.co/planes-estrategicos-sectoriales-e-institucionales):
- El plan no cuenta con la estructura de forma establecida para los documentos SIG de la entidad.
- El documento refiere los lineamientos generales establecidos en el Modelo de Seguridad y Privacidad de la información (MINTIC y Vive Digital Colombia); no obstante, no se identifica de manera clara cuales son los lineamientos de buenas prácticas en Seguridad y Privacidad propias establecidas para la entidad.
- No se identifica de manera clara como se cumplen los objetivos específicos establecidos en el documento o los aspectos diferenciadores para la entidad respecto al modelo de MINTIC
- El documento no identifica los plazos para ejecutar las metas propuestas, por lo tanto se dificulta llevar a cabo la evaluación de la oportunidad de su ejecución.

2.3. Plan de Seguridad y Privacidad de la Información 2020, publicado en la página web ((https://www.fuga.gov.co/planes-estrategicos-sectoriales-e-institucionales):
- El documento publicado no refiere políticas de operación. En este campo se indica la instrucción de la información que allí debe registrarse

- Las metas son genéricas y las actividades descritas para cada una de ellas no son claras y evidencian debilidades de redacción (*En esta fase se pretende identificar…; Esta fase le permitirá a la entidad…*; entre otras) (Subrayado fuera de texto)
- No se identifica de manera clara como se articulan las metas con los plazos establecidos para implementar el Modelo Seguridad y Privacidad de la Información.
- La formulación de los indicadores está mal planteada (La base se está tomando como numerador y lo ejecutado como denominador)

Adicionalmente se recomienda publicar en formatos de datos abiertos

2.4. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2019 - Versión1, publicado en la página web ((https://www.fuga.gov.co/planes-estrategicos-sectoriales-e-institucionales):

- El documento no tiene el estándar de los documentos SIG de la entidad
- El documento refiere los lineamientos generales establecidos en la *Guía para la administración del riesgo y el diseño de controles en entidades públicas* del DAFP); no obstante, no se identifica de manera clara cuales son los lineamientos propios establecidos para la entidad.

2.5. Plan de tratamiento de Riesgos SGSI y su tratamiento – 2019, publicado en la página web ((https://www.fuga.gov.co/planes-estrategicos-sectoriales-e-institucionales):

- El documento corresponde Anexo 1. *Matriz plan de tratamiento de riesgos de seguridad de la información – formato Excel*, que se incluye en el *Plan de Tratamiento de Riesgos de Seguridad y Privacidad de a información*, citado en el ítem anterior. La matriz no identifica el nombre de entidad.

2.6. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2020, publicado en la página web ((https://www.fuga.gov.co/planes-estrategicos-sectoriales-e-institucionales):

- El documento publicado no refiere políticas de operación. En este campo se indica la instrucción de la información que allí debe registrarse
- El nombre del plan no corresponde con lo indicado (El documento publicado indica que el nombre del plan es PLAN DE TRATAMIENTO DE SEGURIDAD DE LA INFORMACIÓN, lo cual es diferente al Plan de Tratamiento de Riesgos).
- No se evidencia de manera clara la articulación de la meta y la actividad 1 del plan
- La formulación de los indicadores está mal planteada (La base se está tomando como numerador y lo ejecutado como denominador)

Adicionalmente se recomienda publicar en formato de datos abiertos

2.7. Plan Estratégico de Tecnologías de la Información y Comunicaciones – PETIC (2019) - GTI-PETIC: Versión 1, publicado en la página web ((https://www.fuga.gov.co/planes-estrategicos-sectoriales-e-institucionales):

- La información correspondiente al numeral iv. Equipos de Cómputo no corresponde con la información remitida para el reporte de Derechos de Autor Software llevado a cabo por la OCI en el 2019, correspondiente a la gestión de la vigencia 2018
- En el numeral 7 Políticas Informáticas Internas y de Seguridad, literal a. Confidencialidad y b. Asignación de recursos: solo hace referencia a contratistas

- Acápite POLITICAS DE SEGURIDAD DE LA INFORMACIÓN: literal a. Copias de seguridad de los datos de los usuarios mensual (los primeros 8 días) difiere de lo indicado en el ítem 7 numeral f. (los primeros 5 días).
- En el numeral 17 Planes de Contingencia, literal a. Copias de seguridad de los sistemas de información, se indica "*copia de seguridad mensual de la información misional de la entidad*" (Subrayado fuera de texto), no se observa cual es el tratamiento relacionado con la información diferente a la misional (Apoyo, estratégica, entre otros)
- En el numeral 18 DIGANOSTICO numeral b. Evaluación externa, el 2o. y 3er párrafo no son amenazas (externas)
- El documento refiere dos subtítulos 7. POLITICAS INFORMÁTICAS INTERNAS Y DE SEGURIDAD y otro sin numeración POLITICAS DE SEGURIDAD DE LA INFORMACIÓN que contienen información similar.

Adicionalmente se recomienda fortalecer los ejercicios de revisión previa a la publicación de los documentos, lo anterior en razón a que se observaron errores de forma o de ortografía: Halla (Página 18 y 26); Numeral 18 DIAGNOSTICO " *... para el mejor servicio del departamento para beneficio de la entidad*" (Subrayado fuera de texto), la FUGA no tiene departamentos en su estructura organizacional; el 2o. párrafo se indica "culturano" y el 3er. párrafo no es claro

2.8. Plan Estratégico de Tecnologías de la Información y Comunicaciones - PETIC (2020 - 2023) Versión 1, publicado en la página web ((https://www.fuga.gov.co/planes-estrategicos-sectoriales-e-institucionales):

- La información correspondiente al numeral iv. Equipos de Cómputo no corresponde con la información remitida para el reporte de Derechos de Autor Software llevado a cabo por la OCI en el 2020, correspondiente a la gestión de la vigencia 2019
- En el numeral 7 Políticas Informáticas Internas y de Seguridad, literal a. Confidencialidad y b. Asignación de recursos: solo hace referencia a contratistas
- Acápite POLITICAS DE SEGURIDAD DE LA INFORMACIÓN: literal a. *Copias de seguridad de los datos de los usuarios se realiza cada semana*, lo cual difiere de lo indicado en el ítem 7 numeral f. (mensualmente los primeros 5 días).
- En el numeral 9 Planes de Contingencia, literal a. Copias de seguridad de los sistemas de información, se indica "*copia de seguridad mensual de la información misional de la entidad*", no se observa cual es el tratamiento relacionado con la información diferente a la misional (Apoyo, estratégica, entre otros)
- En el numeral 10 DIGANOSTICO numeral b. Evaluación externa, el 2o. y 3er párrafo no son amenazas (externas)
- El documento refiere dos subtítulos 7. POLITICAS INFORMÁTICAS INTERNAS Y DE SEGURIDAD y otro sin numeración POLITICAS DE SEGURIDAD DE LA INFORMACIÓN que contienen información similar
- En la introducción, 3er. párrafo hace referencia al periodo del plan de 2016-2020
- Los literales del ítem POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN inician en la letra b.

Adicionalmente se recomienda ffortalecer los ejercicios de revisión previa a la publicación de los documentos, lo anterior en razón a que se observaron errores de forma o de ortografía: Halla (Página 18 y 26); Numeral 10 DIAGNOSTICO " ... *para el mejor servicio del departamento para beneficio de*

la entidad" (Subrayado fuera de texto), la FUGA no tiene departamentos en su estructura organizacional; el 2o. párrafo se indica "culturano" y el 3er. párrafo no es claro

2.9. Políticas de Seguridad de la Información (GTI-POL-01) Versión 1, publicado en la página Intranet - Centryfuga (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)

- El documento publicado en la página web link de Transparencia, ítem *1.4. Políticas de seguridad de la información y protección de datos personales* no se encuentra actualizado conforme la versión publicada en la intranet (http://intranet.fuga.gov.co/sites/default/files/gt-po-01_politicas_seguridad_de_la_informacion_v2_20022020.pdf)
- Los numeral 6.5, 6.6, 6.7, 6.8 y 6.9 son subnumerales del 6.5

2.10. Caracterización Gestión de Tecnologías de la Información (GTI-CA) Versión 3, publicado en la página Intranet - Centryfuga (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)

- De acuerdo a la información aportada por el proceso, se evidencia que la caracterización no ha sido actualizada.

2.11. Guía para la administración de activos de la información (CEM-GU-01) Versión 2, publicado en la página Intranet - Centryfuga (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)

- No es clara la redacción del objetivo de la guía
- El Alcance no es claro, no identifica el inicio y final
- La Normatividad Específica no presenta la información de conformidad con el estándar de las normas APA.
- Las responsabilidades definidas son genéricas (Para todos los funcionarios).
- No se da cumplimiento a lo establecido en el segundo párrafo del ítem 6 GENERALIDADES y la redacción inicial del mismo no permite entender de manera clara su contexto: *"Estar al tanto la criticidad de los activos información de la entidad con el fin de darle el trato adecuado, de esta manera mitigar los riesgos de seguridad de la información a los que se puedan exponer, este registro de información se debe actualizar en los portales web designados como mínimo una vez al año"* (subrayado fuera de texto)
- Los ítems relacionados con los activos tipo definen de manera general los conceptos macro, no obstante, no se evidencia la especificidad vinculada a la entidad, con excepción de los activos tipo colección biblioteca especializada y colección obras de arte
- El primer párrafo del ítem *8 Políticas para el uso aceptable de los activos*, no es claro cuál es el **deben**. *"Las actividades referentes a la administración, uso, operación que se ejecuten en los activos de información deben con el fin de garantizar el correcto cumplimiento de la misión de la Fundación Gilberto Álzate."* (subrayado fuera de texto)
- En el último párrafo del ítem *8 Políticas para el uso aceptable de los activos*, se establece el lineamiento de: "*Ningún funcionario deberá compartir usuarios y contraseñas de los sistemas de información.*", no obstante conforme lo estipulado en las Políticas de Seguridad de la Información (GT-PO-01) versión1: "*No socialice ni comparta su clave bajo ningún motivo*", se debería clasificar como un Uso no autorizado

2.12. Procedimiento Actualización del Plan Estratégico de Tecnologías de Información y Las Comunicaciones - PETIC, (GT-PD-01) Versión1, publicado en la página Intranet - Centryfuga (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)

- No son claras las entradas de información y su relación e importancia frente al PETIC (Actividad 1 - Levantar información preliminar)
- No es claro cómo se determina si la información es suficiente. (Actividad 2 Analizar la información)
- No es claro cómo se determina la alineación con la normatividad (Actividad 3 Revisar y actualizar la modelación integral del centro de Datos y Cómputo de la Entidad)
- No es claro cómo se definen los planes de acción y la relación con las actividades: Priorizar los proyectos e identifica la importancia de la ejecución para la entidad; Plasmar en el PETIC los planes y proyectos de tecnología a desarrollar; y Consolidar el documento final PETIC (Actividad 4. Identificar y definir planes de acción y proyectos asociados al PETIC).
- No es claro cuándo se remitió a la Subdirectora de gestión corporativa y sobre qué se deben basar sus comentarios y aprobación. (Actividad 5. Formular versión inicial del PETIC)

Adicionalmente se realizan las siguientes recomendaciones:

- Vincular con procedimiento de comunicaciones (Actividad 7. Solicitar publicación y divulgación del PETIC)
- Incluir la aprobación del comité directivo sobre las modificaciones (Actividad 8. Modificar el PETIC)
- Incluir que el seguimiento se presente a la Alta Dirección para toma de decisiones (Actividad 10. Hacer seguimiento al PETIC)

2.13. Procedimiento Gestión de soluciones y servicios de tecnología -Mesa de ayuda (GT-PD-02) Versión 2, publicado en la página Intranet - Centryfuga (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)

- Actividad 2 (Visitar en sitio) y 3 (Dar solución en sitio) se describen de forma similar

Adicionalmente se realizan las siguientes recomendaciones:

- Detallar cómo se hace el análisis de prioridad de las solicitudes y los criterios para el tiempo de atención. (Actividad 1 1. Tramitar las solicitudes por GLP)
- Verificar si siempre se realiza visita en sitio (no es coherente con actividad anterior). (Actividad 2. Visitar en sitio)

2.14. Procedimiento Gestión de soluciones y servicios de tecnologías (GT-PD-03) Versión 1, publicado en la página Intranet - Centryfuga (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)

- No es claro el objetivo "*Alinear los servicios y soluciones de tecnología de la información para apoyar el cumplimiento de los objetivos misionales conforme al avance tecnológico y las necesidades que se presenten en la Fundación Gilberto Alzate Avendaño*" (Subrayado fuera de texto)
- No es clara la secuencia de la actividad 4: *Realizar mantenimiento correctivo: Los ingenieros y/o proveedores contratados deben velar por el funcionamiento correcto del software y el hardware en caso de que haya una operación errónea de algún medio TIC se debe Realizar mantenimiento correctivo a la solución tecnológica en el caso que aplique a través de inspecciones y revisiones de logs de sistemas*
- No es claro el control que efectúa ni cómo se determina el éxito de las pruebas (Actividad 6. Realizar pruebas de mantenimiento)

- El procedimiento no puede culminar si se hace referencia a una toma de decisión, se recomienda incluir las acciones que continúan.

Adicionalmente se realizan las siguientes recomendaciones:

- Verificar si los mantenimientos correctivos se pueden planear en cronograma (Políticas de Operación)
- Relacionar en el procedimiento cuál es la función del comité y la finalidad de socializar la documentación (Actividad 2. Socializar la documentación frente al comité de desempeño y determinar su grado de utilidad de servicio y de obsolescencia)
- Detallar cuándo se utiliza cada revisión (Actividad 3. Realizar seguimiento al funcionamiento de las soluciones tecnológicas a nivel de software o hardware)
- Verificar redacción de la actividad 5. Realizar mantenimiento preventivo

2.15. Procedimiento Asignación de cuentas (GT-PD-04) Versión 1, publicado en la página Intranet - Centryfuga (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)

- Conforme se encuentran redactadas las políticas de operación, estas corresponden a actividades dentro del procedimiento
- El detalle de la actividad *2. Asignar equipos y creación de cuentas* no corresponde a lo anunciado

Adicionalmente se realizan las siguientes recomendaciones:

- No establecer como objetivo del procedimiento "*establecer actividades*" es el objetivo del documento.
- Verificar la redacción del Punto de Control (PC) por cuanto no se identifica que se debe verificar
- No es clara la redacción de la actividad *3. Acceso a sistemas de información*, se recomienda especificar para qué se establece el Punto de Control (PC)

2.16. Procedimiento Respaldo de la información (GT-PD-05) Versión1, publicado en la página Intranet - Centryfuga (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)

- Conforme se encuentran redactadas las políticas de operación, estas corresponden a actividades dentro del procedimiento
- El detalle de la actividad *2. Asignar equipos y creación de cuentas* no corresponde a lo anunciado
- No es clara la redacción de la actividad *1. Programar el respaldo* y del Punto de control (PC). De igual manera no se evidencia el Anexo *Tabla frecuencias mínimas para el respaldo de información*.
- No es clara la secuencia en el procedimiento establecido en la actividad *2. Evaluar impactos*
- No es claro el Punto de Control (PC) establecido para la actividad 3. Realizar pruebas de recuperación
- No es clara la actividad *4. Realizar control*

Adicionalmente se realizan las siguientes recomendaciones:

- No establecer como objetivo del procedimiento "*establecer actividades*", es el objetivo del documento.
- Verificar redacción de la política de operación "*Cada respaldo que se realice deberá quedar registrado en los logs de los servidores. Archivos a copiar Sólo copiar los ficheros que se hayan modificado o movido*"

- No se identifica de manera clara en la política de operación "*La información que no sea relevante para la institución no será respaldada, de acuerdo a lo que establezca la Subdirección gestión corporativa en la política de seguridad que se encuentra publicada y divulgada*" quién cómo y dónde se establece qué información es relevante por lo que se recomienda hacer referencias cruzadas con las políticas y demás documentos que lo señalen

2.17. Procedimiento Implementación de soluciones y servicios de Tecnología (GT-PD-06) Versión1, publicado en la página Intranet - Centryfuga (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)

- No es clara la política de operación pues existe un procedimiento para actualizar PETIC

Adicionalmente se realizan las siguientes recomendaciones:

- Verificar el objetivo con relación a los demás procedimientos, pues no es perceptible por su redacción las diferencias de los mismos.
- Verificar el procedimiento pues relaciona actividades contractuales y del procedimiento relacionado con PETIC

2.18. Procedimiento Operaciones del centro de datos (GT-PD-03) Versión 1, publicado en la página Intranet - Centryfuga (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)

- Si bien el documento del archivo se identifica con el nombre gt-pd-07, internamente el código asignado es GT-PD-03, el cual coincide con el Procedimiento de Soluciones y Servicios.
- Las políticas de operación deben contener directrices específicas como, cuando y quién; condiciones que no se evidencian en las definidas.

Adicionalmente se realizan las siguientes recomendaciones:

- No establecer como objetivo del procedimiento "*establecer actividades*" es el objetivo del documento.
- Se recomienda verificar si este documento corresponde a la finalidad de un procedimiento o un instructivo

2.19. Procedimiento Sistemas operativos de Servidores – Estaciones (GT-PD-08) Versión 1, publicado en la página Intranet - Centryfuga (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)

- En la política de operación "*No se podrán realizar intervenciones a los equipos, salvo las estrictamente necesarias*." (Subrayado fuera de texto) no se indican cuáles son las estrictamente necesarias

Adicionalmente se realizan las siguientes recomendaciones:

- No establecer como objetivo del procedimiento "*establecer actividades*" es el objetivo del documento.
- Se recomienda verificar si este documento corresponde a la finalidad de un procedimiento o un instructivo
- Validar en la revisión previa a la publicación, la completitud de los campos de los formatos; lo anterior en razón a que el campo que corresponde al nombre *Políticas de Operación* no se encuentra diligenciado.

2.20. Procedimiento Gestión de incidentes, amenazas y debilidades de seguridad (GT-PD-03) Versión 1, publicado en la página Intranet - Centryfuga (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)

- Si bien el documento del archivo se identifica con el nombre gt-pd-09, internamente el código asignado es GT-PD-03, el cual coincide con el Procedimiento de Soluciones y Servicios.
- No es clara la secuencia de acciones en la actividad *1. Identificar los activos*
- No es claro el PC y su relación con la actividad (Actividad 4. Registrar incidentes y/o amenazas)

Adicionalmente se realizan las siguientes recomendaciones:

- No establecer como objetivo del procedimiento "*establecer actividades*" es el objetivo del documento
- Incluir para qué se informa a la Dirección (Actividad 3. Dar respuesta ante incidentes, amenazas y debilidades de seguridad)
- No es claro el cómo se vela por el acceso lógico al punto de acceso inalámbrico (WIFI) (Actividad 5), se recomienda revisar si es una política de operación

2.21. Procedimiento Seguridad de redes (GT-PD-10) Versión 1, publicado en la página Intranet - Centryfuga (http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia)

- Las políticas de operación deben contener directrices específicas como, cuando y quién; condiciones que no se evidencian en las definidas.
- No es claro el punto de control (PC) y su relación con la actividad *4. Administrar acceso remoto (VPN*)
- No es claro el punto de control (PC) y su relación con la actividad *5. Cambiar contraseña acceso inalámbrico (WIFI)*; está redactado como política de operación

Adicionalmente se realizan las siguientes recomendaciones:

- No establecer como objetivo del procedimiento "*establecer actividades*" es el objetivo del documento
- Se recomienda verificar si este documento corresponde a la finalidad de un procedimiento o un instructivo

Por último, es importante señalar que de la verificación realizada, se evidenciaron documentos publicados en la página web, que no hacen parte de los documentos SIG del proceso:

- Política de tratamiento de la información y protección de datos personales
- Políticas internas de Seguridad y tratamiento de datos
- Políticas web tratamiento de datos
- Manual recomendaciones de seguridad
- Protocolo de atención a titulares información

Sin embargo, estos si se incorporan como parte de la ejecución en la fase de implementación del MSPI, evaluada a continuación.

3. Verificación del nivel de madurez de la implementación del Modelo de Seguridad y Privacidad de la Información.

Como resultado de la aplicación del Instrumento Evaluación MSPI sugerido por MINTIC, se observa el siguiente nivel de madurez respecto a su implementación

3.1. Evaluación de Efectividad de Controles – ISO 27001:2013 Anexo A:

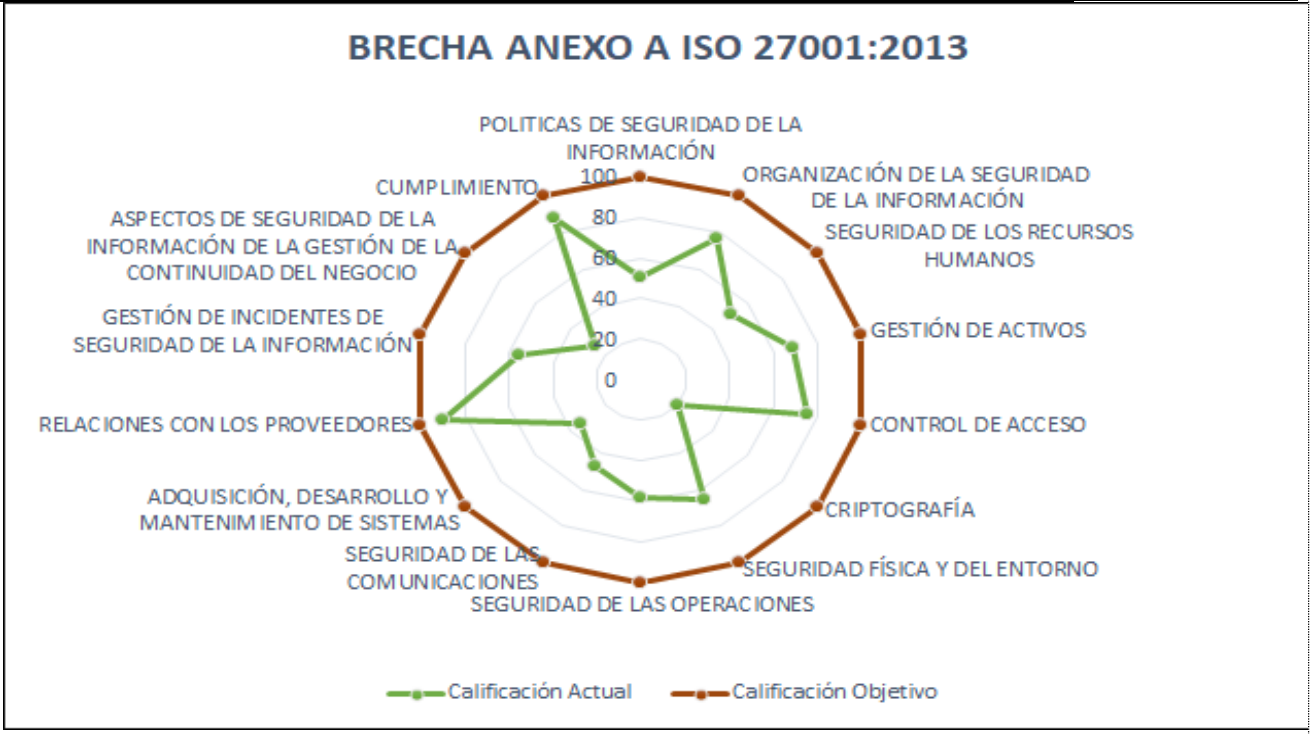
Se aplicó la siguiente escala de valoración, conforme establece el instrumento:

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Una vez verificados los documentos vinculados al proceso Gestión de Tecnologías (Planes, Políticas, Protocolos, Guías, Manuales y Procedimientos), las evidencias aportadas y la aplicación de las listas de verificación a los responsables operativos del proceso; se procedió a evaluar los componentes Administrativo y Técnico del instrumento, cuyo resultado se presenta a continuación:

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50	100	**EFECTIVO**

A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	77	100	**GESTIONADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	51	100	**EFECTIVO**
A.8	GESTIÓN DE ACTIVOS	69	100	**GESTIONADO**
A.9	CONTROL DE ACCESO	75	100	**GESTIONADO**
A.10	CRIPTOGRAFÍA	20	100	**INICIAL**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	65	100	**GESTIONADO**
A.12	SEGURIDAD DE LAS OPERACIONES	58	100	**EFECTIVO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	47	100	**EFECTIVO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	34	100	**REPETIBLE**
A.15	RELACIONES CON LOS PROVEEDORES	90	100	**OPTIMIZADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	56	100	**EFECTIVO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	27	100	**REPETIBLE**
A.18	CUMPLIMIENTO	88,5	100	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**58**	**100**	**EFECTIVO**

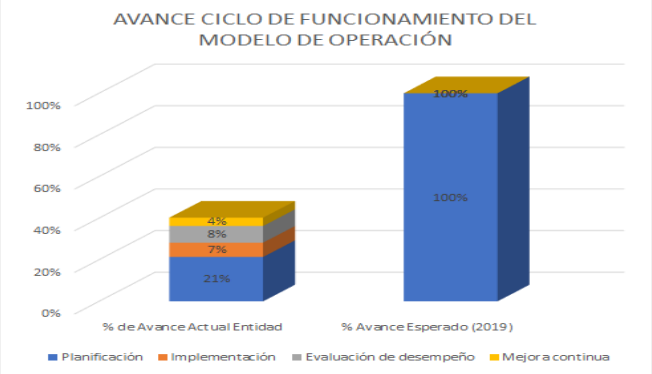


Lo anterior y conforme la Escala de Valoración, se observa que en la entidad *"Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada"*

Cada uno de los criterios evaluados, observaciones y recomendaciones de la OCI se presentan en el documento Anexo 4 Instrumento Evaluación MSPI (Hojas Administrativa y Técnicas), el cual hace parte integral del presente informe

3.2. Avance Ciclo de Funcionamiento del Modelo de Operación (PHVA):

AVANCE PHVA		
COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
Planificación	**21%**	100%
Implementación	**7%**	100%
Evaluación de desempeño	**8%**	100%
Mejora continua	**4%**	100%



Cada uno de los criterios evaluados, observaciones y recomendaciones de la OCI se presentan en el documento Anexo 4 Instrumento Evaluación MSPI (Hoja PHVA), el cual hace parte integral del presente informe

3.3. Nivel de Madurez Modelo Seguridad y Privacidad de la Información:

Conforme lo registrado en los componentes Administrativo, Técnico y PHVA y en la siguiente escala de evaluación, la cual se aplica de manera automática en el instrumento de evaluación:

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Se observa el siguiente nivel de madurez del MPSI:

		NIVEL DE CUMPLIMIENTO	CONTEO DE VALORES IGUAL A MENOR	TOTAL DE CALIFICACIONES DE CUMPLIMIENTO
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	**Inicial**	SUFICIENTE	0	10
	Repetible	SUFICIENTE	3	21
	Definido	INTERMEDIO	16	42
	Administrado	CRÍTICO	40	59
	Optimizado	CRÍTICO	53	60

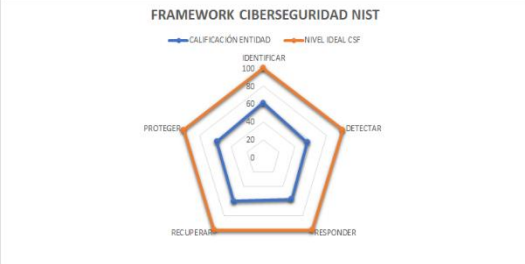
De acuerdo a la valoración de los 192 criterios evaluados se observa que la entidad se encuentra en un nivel INTREMDIO de madurez. (El 42% de los requisitos se califican con cumplimiento)

3.4. Calificación frente a mejores prácticas en Ciberseguridad (NIST):

Conforme la evaluación realizada en los componentes Administrativo, Técnico, PHVA y Ciberseguridad, el Instrumento de evaluación clasifica conforme los siguientes temas:

- **Identificar:** Gestión de activos, Ambiente de Negocios, Evaluación de Riesgos y Estrategia de gestión de riesgos
- **Proteger:** Control de acceso, Capacitación y Sensibilización, Seguridad Datos, Protección Información y procedimientos, Mantenimiento y Tecnología de Protección
- **Detectar:** Anomalías y eventos, Monitoreo continuo de la seguridad y Proceso de detección
- **Responder**: Planes de respuesta, Comunicaciones, Análisis, Mitigación y Mejoras.
- **Recuperarse**: Planes de recuperación, Mejoras y Comunicaciones

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
FUNCION CSF	**CALIFICACIÓN ENTIDAD**	**NIVEL IDEAL CSF**
IDENTIFICAR	61	100
DETECTAR	56	100
RESPONDER	59	100
RECUPERAR	60	100
PROTEGER	59	100



4. Gestión de Riesgos:

De acuerdo a la verificación del Mapa de Riesgos por Procesos vigente para el 2019, se evidencia que el proceso Gestión de Tecnología, tiene identificado 4 riesgos así:

- Pérdida de información almacenada en medios tecnológicos: Zona de Riesgos Inherente Alta – Zona de Riesgo Residual: Media
- Interrupción de los servicios de red: Zona de Riesgos Inherente Alta – Zona de Riesgo Residual: Media
- Daño en los recursos tecnológicos: Zona de Riesgos Inherente Alta – Zona de Riesgo Residual: Alto
- Ataques cibernéticos a los aplicativos: Zona de Riesgos Inherente Alta – Zona de Riesgo Residual: Media

Teniendo en cuenta que no se actualizó el mapa de riesgos durante de la vigencia, se mantiene lo observado por la OCI en el informe de marzo de 2019 de seguimiento a la gestión de riesgos, donde se identificaron las entre otras, siguientes debilidades:

- Los riesgos tipificados como de Seguridad Digital (Pérdida de información almacenada en medios y tecnológicos, Daño en los recursos tecnológicos y Ataques cibernéticos a los aplicativos), no identifican de manera clara si corresponde a la perdida de confidencialidad, de la integridad o de la disponibilidad de los activos; así como tampoco se evidencia la realización en la entidad, de la Identificación de Activos tal como se establece en la "Guía para la Administración del riesgo y el diseño de controles en entidades públicas (Versión 4, Octubre de 2018)." y en el Anexo 4 "Lineamientos para la Gestión del Riesgo de Seguridad Digital en entidades públicas"
- Adicionalmente la matriz implementada de Riesgos no considera los aspectos relacionados con el Activo asociado al riesgo de Seguridad Digital identificado, así como la amenaza vinculada para cada uno de ellos
- No hay evidencias de la metodología empleada en la identificación de causas/vulnerabilidades
- No se identifican causas/vulnerabilidades que correspondan a factores externos (Contexto Externo) que pueden afectar el logro del objetivo.
- No se evidencia la identificación de riesgos relacionados con el uso no autorizado de licencias y/o software, ni riesgos de privacidad en el Mapa de Riesgos Por Procesos publicado por la entidad.
- La causa "Daño de los recursos tecnológicos", podría corresponder más a una consecuencia de un ataque cibernético que a una causa.
- No se encuentran registros del análisis de frecuencia y factibilidad de los riesgos identificados
- La calificación de impacto no es coherente con las consecuencias identificadas para cada uno de los riesgos identificados.
- No se identifican planes de contingencia para los riesgos: Pérdida de información almacenada en medios tecnológicos y Ataques cibernéticos a los aplicativos
- El establecimiento de formatos, procedimientos o políticas no aseguran su uso, por lo tanto no son controles por si mismos, ni reducen el riesgo.
- No se identifica la relación directa de los controles existentes para mitigar todas las causas identificadas.
- El formato establecido en el Mapa de Riesgos no define el responsable de llevar a cabo la ejecución de los controles, así como su periodicidad. No indica propósito ni desviaciones.
- La valoración de controles no se está haciendo según los lineamientos de la Guía para la administración de riesgos 2018 adoptada por la Entidad como lineamiento para la administración de riesgos.

- Dentro de los controles actuales identificados, se describen actividades que no permiten verificar, validar, conciliar, cotejar, comparar, entre otros, propósitos específicos de los controles.

5. Gestión PQRS

De acuerdo a la verificación realizada por el equipo auditor a los informes de seguimiento semestrales a la gestión de PQRS de la entidad y de acuerdo a la confirmación del Profesional Universitario responsable de Gestión Documental y Atención al Ciudadano, en el periodo auditado se recibieron 3 peticiones así:

- Entrada 20192300001212 - Respuesta 20192900002681
- Entrada 20192300003102 - Respuesta 20192900004431
- Entrada 20192300003862 - Respuesta vía correo electrónico adjunto al radicado de entrada.

Las cuales fueron atendidas por el equipo de TI dentro de los términos establecidos.

6. Matriz de Cumplimiento Legal:

De acuerdo a la verificación realizada por el equipo auditor a la Matriz de Cumplimiento Legal recibido como evidencia, se hacen las siguientes observaciones:

FUGA ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE	Proceso:	Control, Evaluación y Mejora
	Documento:	Matriz de Cumplimiento Legal
	Fecha de aprobación:	15 de noviembre de 2016

TEMÁTICA	CLASIFICACIÓN NORMATIVA	AÑO	EPIGRAFE	ARTÍCULO APLICABLE	REQUERIMIENTO ESPECÍFICO	SUBSISTEMA NTD-SIG	PROCESO	FRECUENCIA DE APLICACIÓN DEL	OBSERVACIÓN OCI
Alcalde Mayor de Bogotá D.C.	Decreto Distrital 680	2001	Por el cual se modifica la Comisión Distrital de Sistemas -CDS-	Todos los artículos	Identificar a la CDS como el ente rector de los sistemas	Gestion de Seguridad de la Información	Gestion TIC	Siempre	Se recomienda incluir la Ley 962 de 2005 *por la cual se dictan 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 públicos*. El artículo 6 trata lo referente a medios tecnológicos para atender trámites y procedimientos
Concejo de Bogotá	Acuerdo 057	2002	Por el cual se dictan disposiciones generales para la implementación del Sistema Distrital de Información - SDI, se organiza la Comisión Distrital de Sistemas, y se dictan otras disposiciones.	Todos los artículos	Estrategia Distrital de Gobierno Electrónico.	Gestión de Seguridad de la Información	Gestion TIC	Cuatrimestral	El Acuerdo 409 de 2009 derogó el artículo 9 del Acuerdo 57 de 2002. Falta incluirlo
Comisión Distrital de Sistemas (CDS) de Bogotá, D.C.	Resolución 305	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,	Todos los artículos	Establecimiento de políticas públicas en tecnologías de la información	Gestión de Seguridad de la Información	Gestion TIC	Cuatrimestral	Falta referenciar la Resolución 256 de 2008 "Por la cual se establece el reglamento interno de la Comisión Distrital de Sistemas – C.D.S. -"

No se incluye en la matriz: Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2. ESTRATEGIA DE GOBIERNO EN LINEA (Gobierno Digital).

7. Gestión Plan de Acción:

Para la vigencia 2019, el proceso Gestión de Tecnologías identifico 11 metas vinculadas al mismo número de actividades, sobre las cuales la OCI al cierre de diciembre, presento las siguientes recomendaciones (Informe Evaluación por Dependencias – 2019, publicado en la página web de la entidad https://www.fuga.gov.co/informes-de-control-interno-2020:

1. Actualizar el PETIC y Gestionar su aprobación:
   - Detallar en las actas las aprobaciones de los planes y si se hacen recomendaciones sobre el mismo.
   - OAP: Asesorar integralmente la formulación de los planes incluyendo los requisitos relacionados con MIPG y demás lineamientos, con el fin de asegurar que se cumplen todos los requerimientos y los seguimientos son coherentes

2. Ejecutar plan de proyectos a implementar para el año 2019 de acuerdo con el PETIC:
   - Verificar el seguimiento de primera línea de defensa pues no es coherente con el análisis y validación hecha por segunda línea de defensa.
   - Validar la integralidad de la retroalimentación periódica de la OAP para evitar incumplimientos o cumplimientos parciales de los planes institucionales.

3. Formular y aprobar el plan tratamiento de riesgos de seguridad y privacidad de la información
   - La metodología no es el producto esperado, desde la OCI se recomienda validar la pertinencia de la misma, teniendo en cuenta que existe un lineamiento nacional, adoptado mediante la política de administración de riesgos de la Entidad, por lo tanto, no es coherente con los lineamientos externos e internos este documento.
   - No es posible generar un plan de tratamiento cuando los riesgos no se han identificado adecuadamente. No se han atendido las recomendaciones hechas por la OCI sobre el particular, se recomienda revisar los informes de seguimiento a riesgos e implementar la guía elaborada por el DAFP.
   - Se recomienda a la segunda línea de defensa articular sus alertas y recomendaciones pues en el seguimiento al plan de acción MIPG se presentan recomendaciones que en este plan no se han tenido en cuenta.

4. Formular y aprobar el plan de seguridad y privacidad de la información
   - Detallar en las actas las aprobaciones de los planes y si se hacen recomendaciones sobre el mismo, así mismo se recomienda validar que el plan cumple con todos los requisitos y lineamientos vigentes.
   - OAP: asesorar integralmente la formulación de los planes incluyendo los requisitos relacionados con MIPG y demás lineamientos, con el fin de asegurar que se cumplen todos los requerimientos y los seguimientos son coherentes.

5. Formular y aprobar el plan de mejoramiento de servicios tecnológicos
   - Detallar en las actas las aprobaciones de los planes y si se hacen recomendaciones sobre el mismo.
   - Validar la fecha de la versión vigente en el plan publicado.

6. Ejecutar las acciones del plan de mantenimiento de servicios tecnológicos según programación para la vigencia 2019
   - Verificar el seguimiento de primera línea de defensa pues no es coherente con el análisis y validación hecha por segunda línea de defensa.
   - Validar la integralidad de la retroalimentación periódica de la OAP para evitar incumplimientos o cumplimientos parciales de los planes institucionales.

7. Ejecutar las actividades del Plan MIPG planeadas para el año 2019 y a cargo del área de tecnologías
   - Cumplir las actividades programadas con las características requeridas. Así mismo es importante mejorar los seguimientos periódicos pues permiten ajustar posibles fallas en la planeación inicial.

8. Ejecutar las acciones correctivas, y de mejora derivadas del plan de mejoramiento por proceso
   - No se presentaron recomendaciones

9. Realizar seguimiento y reportar los indicadores de gestión según la frecuencia de medición del indicador.
   - No se realizó la medición atendiendo los lineamientos frente al tema, por lo tanto, se sugiere revisarlos y cumplirlos en las actividades que se realicen en la vigencia 2020.
   - OAP: unificar los criterios de seguimiento interno oportunamente para poder brindar asesorías integrales a los procesos frente a todos los temas que lidera.

10. Monitorear los riesgos del proceso.
    - No se realizaron los monitoreos atendiendo los lineamientos frente al tema, por lo tanto, se sugiere revisarlos y cumplirlos en las actividades que se realicen en la vigencia 2020.
    - Mejorar la formulación de la acción pues el indicador no es coherente con la actividad descrita, así mismo el seguimiento corresponde a las acciones de control y no monitoreos.
    - OAP: unificar los criterios de seguimiento interno oportunamente para poder brindar asesorías integrales a los procesos frente a todos los temas que lidera.

11. Gestionar la actualización del link de transparencia de la página web (publicar información) de acuerdo con el esquema de publicación, de los procesos a cargo del área
    - La OCI en el informe de seguimiento al cumplimiento de la ley de transparencia determinó que la Entidad ha cumplido con el 86,57%, por lo tanto, se recomienda publicar la información de forma rutinaria y permanente, con el fin de garantizar el principio de la divulgación proactiva establecido en la Ley de Transparencia.
    - Garantizar el cumplimiento de las acciones propuestas en el Plan y establecer las acciones correctivas pertinentes.

Conforme lo anterior se observa que el promedio de ejecución del POA para la vigencia 2019 fue del 88.75%

De la verificación realizada por el equipo auditor a los documentos del servidor (\\192.168.0.34\plan operativo integral\SUB. GESTIÓN CORPORATIVA\2020\Planes2020\PLAN DE ACCIÓN) se evidencia que el POA para la vigencia 2020 del proceso de Gestión de Tecnologías identifica 12 metas, de las cuales 10 son iguales o similares a las formuladas en la vigencia 2019, por lo que se aplican las recomendaciones indicadas en el ítem anterior.

Las actividades nuevas hacen referencia a:

- Desarrollar el 100 % de actividades de intervención para el mejoramiento de la infraestructura administrativa; en el marco del proyecto de inversión 7032
- 80% del plan de tratamiento de riesgos de seguridad y privacidad de la información ejecutado

8. Gestión Planes de Mejoramiento:

De lo observado en el Plan de Mejoramiento por Procesos 2017 – 2019, se evidencia que el proceso de Gestión de Tecnología no tiene formuladas acciones de mejora.

Conforme lo anterior se evalúa la gestión realizada por el proceso respecto a las recomendaciones realizadas por la OCI en el informe de Derechos de Autor 2018, observándose que se atendieron integral o parciamente las siguientes:

- *Actualizar, de conformidad con la normatividad vigente, los documentos SIG (Procedimientos, Políticas, Planes, Formatos, entre otros) asociados al Proceso Gestión Tecnología de la Información y al Subsistema de Seguridad de la Información.*

  De acuerdo a la información publicada en la intranet y a la evidencia aportada por el proceso, se observa que, con excepción de la Caracterización, la Guía para la Administración de Activos de la Información y las Políticas de Seguridad de la Información; los documentos SIG para el periodo evaluado, fueron actualizados en el mes de diciembre de 2019

- *Dar cumplimiento integral a lo establecido en el Procedimiento para el Monitoreo del Uso de Medios de Procesamiento de Información GTI-PD-04 Versión 1 de fecha 03/02/2016. Actividad 1: Realizar el inventario de medios de procesamiento (dispositivos, computadores, y si como de las licencias, etc.) de propiedad de la entidad.*

  De acuerdo a lo observado y a la actualización de procedimientos realizado por el proceso, se evidencia que este procedimiento fue eliminado.

- *Normalizar, aprobar y publicar en la página web de la entidad los documentos definitivos relacionados con la Gestión de Tecnología; lo anterior en razón a que de la verificación realizada al Plan de Seguridad y Privacidad de la Información - PSPI, Plan estratégico de tecnologías de Información y comunicaciones y Plan de mantenimiento de servicios tecnológicos publicados en el link de Transparencia de la entidad, estos corresponden a documentos en borrador que incluyen observaciones de revisión y no tienen los estándares de imagen institucional de la FUGA*.

  Se observa que los documentos publicados en la página web (https://www.fuga.gov.co/planes-estrategicos-sectoriales-e-institucionales), corresponden a:

  Gestión de Tecnologías y Comunicaciones (TICS)

  Plan estratégico de tecnologías de Información y comunicaciones (PETIC)
  Plan de Tratamiento de Riesgos de Seguridad y Privacidad en la Información
  Plan de tratamiento de Riesgos SGSI y su tratamiento

Plan de Seguridad y Privacidad de la Información (PSPI)
Plan de mantenimiento de servicios tecnológicos

Si bien estos se encuentran actualizados es importante indicar que aún persisten debilidades en cuanto su forma y contenido, los cuales se describen de manera detallada en el ítem 2 del presente informe

DESCRIPCIÓN DE HALLAZGOS

No.	Requisito	Descripción hallazgo
1	Decreto 1078 de 2015 Artículo 2.2.9.1.2.2 Instrumentos - Marco de referencia de arquitectura empresarial para la gestión de Tecnologías de la Información – Política de Gobierno Digital - G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI Guía técnica Versión 1.0	Cumplimiento parcial de los lineamientos establecidos en el PETI expuestos en los numerales 1.1, 2.7 y 2.8 del presente informe
2	Plan de Tratamiento de Riesgos de Seguridad y Privacidad en la Información Anexo 4 *Lineamientos para la Gestión de Riesgos de Seguridad Digital en entidades Púbicas* de MINTIC, Viceministerio de Economía Digital y Dirección de Gobierno Digital	• No se identifican en la Política de Administración de Riesgo de la entidad (CEM-PO-01) Versión 2, los criterios establecidos en los numerales 4.1.2, 4.1.4, 4.1.6 y 4.1.7 del anexo 4 *Lineamientos para la Gestión de Riesgos de Seguridad Digital en entidades Púbicas* de MINTIC. • El Mapa de Riesgos de la entidad no integra en su totalidad los riesgos identificados por el Proceso en el Plan de Tratamiento de Riesgos y no cumple con todos los aspectos identificados para este tipo de riesgos en *el Guía para la administración del riesgo y el diseño de controles en entidades públicas* del DAFP
3	Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información Pública)	No se encuentran publicados los siguientes documentos: • Plan de mantenimiento de servicios Tecnológicos vigencia 2020 • Anexo 1 del Plan de Mantenimiento Infraestructura Tecnológica (Cronograma de mantenimiento Infraestructura Física) de la vigencia 2019 El documento publicado Políticas de Seguridad de la Información se encuentra desactualizado
	Decreto 1078 de 2015 Artículo 2.2.9.1.3.2. y Decreto 2573 de 2014 Artículo 10: Plazos. ISO 27001:2013 Anexo A	De conformidad con el resultado de la evaluación realizada al nivel de madurez del modelo de seguridad y privacidad de la información (MSPI), se observó que no se implementaron los plazos establecidos por MINTIC y Gobierno en Línea; lo

4		anterior teniendo en cuenta que los siguientes criterios presentan debilidades respecto al cumplimiento de los requisitos establecidos para cada uno de ellos. (Calificación por debajo de 40) • A 10: Criptografía • A 14: Adquisición, desarrollo y mantenimientos de sistemas • A 17: Aspectos de seguridad de la información de la gestión de continuidad del negocio De igual forma se observaron controles cuyos requisitos se cumplen con una calificación entre 40 y 70 puntos: • A.5: Políticas de Seguridad de la Información • A 6: Organización de la seguridad de la información • A.7: Seguridad de los recursos Humanos • A 8: Gestión de Activos • A 9: Control de Acceso • A 11: Seguridad Física y del Entorno • A 12: Seguridad de las operaciones • A 13: Seguridad de las comunicaciones • A 16: Gestión de Incidentes de Seguridad de la Información

RECOMENDACIONES GENERALES

- Fortalecer la gestión documental de los planes, de tal manera que haya trazabilidad e integralidad en los soportes que dan cuenta de lo planteado en los mismos (Estrategias, proyectos, actividades, entre otros).
- Teniendo en cuenta que cada uno de los 21 documentos evaluados identifican debilidades respecto a: estructura, forma y fondo que son detallados de manera específica en el ítem 2*. Revisión documental de las guías, procedimientos, políticas y demás documentos SIG, vinculados al Proceso de Gestión de Tecnologías*, del presente informe, se recomienda validar y ajustar de conformidad con lo establecido en la Guía para la Formulación y Seguimiento a Planes Institucionales y Estratégicos (GE-GU-01) y el Procedimiento Formulación, seguimiento y evaluación de planes institucionales y estratégicos (GE-PD-03)
- Fortalecer la gestión documental asociada a la ejecución de los controles establecidos en el Anexo A de la ISO 27001:2013
- Fortalecer la ejecución de las acciones que permitan a la entidad presentar un mayor avance en el ciclo de funcionamiento del modelo de operación (PHVA) del MSPI
- Actualizar la Matriz de Cumplimiento Legal
- Evaluar las recomendaciones realizadas por la OCI en el informe de Evaluación de Dependencias vigencia 2019, a efectos de identificar las correcciones y las oportunidades de mejora que permita al proceso garantizar una efectividad del 100% al cumplimiento del Plan de Acción formulado para la vigencia 2020

- Fortalecer el equipo de trabajo del proceso por cuanto si bien la FUGA no es una entidad robusta en materia de TIC, si está obligada a cumplir con todos los requerimientos normativos establecidos por MINTIC y Gobierno Digital.
- De la verificación realizada al Manual de Funciones de la entidad se observa que no hay definidas funciones vinculadas al proceso evaluado; teniendo la guía No. 4 Roles y Responsabilidades de MINTIC, se recomienda formalizar las responsabilidades del proceso dentro de la estructura orgánica de la entidad

Si bien se realizan las recomendaciones generales, es importante que el proceso auditado evalúe las recomendaciones particulares realizadas en cada uno de los temas desarrollados en este ejercicio de auditoria, con el fin de aportar a la mejora continua del mismo.

FICHA TECNICA

Herramientas Utilizadas:

- Lista de Verificación
- Actas de Reunión
- Instrumento Evaluación MSPI (MINTIC)
- \\192.168.0.34\plan operativo integral\OFICINA ASESORA DE PLANEACIÓN\Plan de Acci Dependencia\Plan de acción por Dep 2019\Evidencias\Subdirección de Gestión Corporativa\TIC
- https://www.fuga.gov.co/planes-estrategicos-sectoriales-e-institucionales
- http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia

Muestra:

N.A

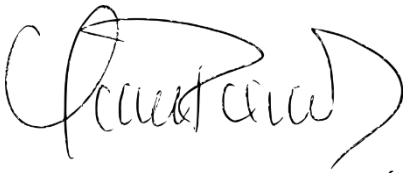
CONCLUSIONES DE AUDITORIA
(La unidad auditable cumple con los requisitos establecidos)

El proceso cumple con los requisitos de eficacia. Presenta oportunidades de mejora en eficiencia y efectividad

Este documento corresponde a los resultados del Informe Preliminar presentado y aprobado mediante acta de fecha 30/04/2020 con el Líder del Proceso Martha Lucia Cardona Visbal y Responsables Operativos Edwin Diaz y Ernesto Ojeda

ANGELICA HERNÁNDEZ RODRÍGUEZ

AUDITOR (Firma)



MARIA JANNETH ROMERO MARTÍNEZ

JEFE OFICINA CONTROL INTERNO (firma)

No. Radicado de entrega:

20201100013513

FECHA ENTREGA	04	05	20

Anexo

SEGUIMIENTO PLAN MEJORAMIENTO AUDITORIA INTERNA VIGENCIA ANTERIOR

Vigencia	***Informe Auditoria Interna Fecha***	***suscripción Plan Mejora Fecha***	***Hallazgo***	***Estado Acción **** *A - C*	***Observación***
* A: Abierta C: Cerrada					

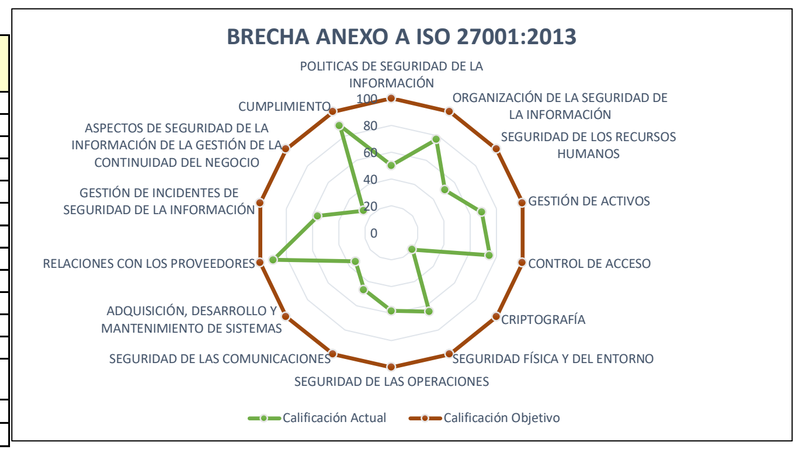
OBSERVACIONES GENERALES PLAN MEJORAMIENTO

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA PORTADA

ENTIDAD EVALUADA	FUNDACIÓN GILBERTO ALZATE AVENDAÑO
FECHAS DE EVALUACIÓN	01/02/2020 - 30/04/2020
CONTACTO	EDWIN DIAZ
ELABORADO POR	María Janneth Romero Martínez

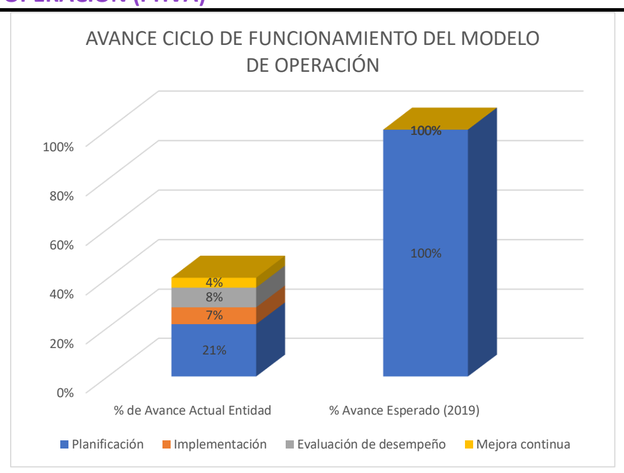
EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	77	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	51	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	69	100	GESTIONADO
A.9	CONTROL DE ACCESO	75	100	GESTIONADO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	65	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	58	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	47	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	34	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	90	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	56	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	27	100	REPETIBLE
A.18	CUMPLIMIENTO	88,5	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		58	100	EFECTIVO



AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado (2019)
2015	Planificación	21%	100%
2016	Implementación	7%	100%
2017	Evaluación de desempeño	8%	100%
2018	Mejora continua	4%	100%
	TOTAL	40%	400%



NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

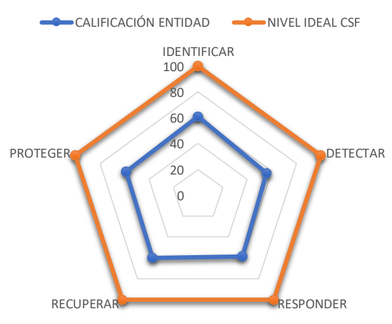
		NIVEL DE CUMPLIMIENTO	CONTEO DE VALORES IGUAL A MENOR	TOTAL DE CALIFICACIONES DE CUMPLIMIENTO	
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Inicial	SUFICIENTE	0	10	10
	Repetible	SUFICIENTE	3	21	18
	Definido	INTERMEDIO	16	42	26
	Administrado	CRÍTICO	40	59	19
	Optimizado	CRÍTICO	52	60	8
			58%	111	192	81	42%

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO				
CRÍTICO	0% a 35%	CRITICO	92	77%
INTERMEDIO	36% a 70%		119	
SUFICIENTE	71% a 100%	INTERMEDIO	16	38%
			42	
		SUFICIENTE	3	10%
			31	
			111	58%
			192	39

CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
FUNCION CSF	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	61	100
DETECTAR	56	100
RESPONDER	59	100
RECUPERAR	60	100
PROTEGER	59	100



INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

FUNDACIÓN GILBERTO ALZATE AVENDAÑO

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN											
AD.1	**Responsable de SI**	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**	**Orientación de la dirección para gestión de la seguridad de la información**	**A.5**	**Componente planificación y modelo de madurez nivel gestionado**					50	
AD.1.1	Responsable de SI	Documento de la política de seguridad y privacidad de la Información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a la partes externas pertinentes	A.5.1.1	Componente planificación y modelo de madurez inicial	ID.GV-1	Solicite la política de seguridad de la información de la entidad y evalúe: a) Si se definen los objetivos, alcance de la política b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección Revise si la política: a)Define que es seguridad de la información b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos; c) Los procesos para manejar las desviaciones y las excepciones. Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas. Verifique cada cuanto o bajo que circunstancias se revisan y actualizan, verifique la ultima fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual. **Para la calificación tenga en cuenta que:** 1) Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, están en 20. 2) Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, , están en 40. 3) Si se divulgan las políticas de seguridad y privacidad de la información, están en 60.	De acuerdo a la información publicada en la entidad a través de la página web y la intranet, se evidencia el documento Políticas de Seguridad de la Información (GT-PO-01 Versión2), con la cual se evalúan los criterios establecidos en este aparte, observándose: a) Objetivo y alcance de la política se encuentran definidos en el documento (Página 8) b) La articulación entre la estrategia y objetivos de la entidad con la política se tratan en el aparte GENERALIDADES (página 5) c) Aprobada en Comité Directivo del 26 de diciembre de 2019, no obstante no se evidencia la socialización del documento y el acta del comité no se encuentra cargada en el ORFEO Adicionalmente se evalúa: a) No se evidencia la definición de Seguridad de la Información b) Se observa que se establecen de manera general las responsabilidades y los roles en las 11 políticas que hacen parte del documento Políticas de Seguridad de la Información (GT-PO-01 Versión2) c) No se identifican los procesos para manejar desviaciones y excepciones. Respecto a quien o quienes son los responsables designados por la dirección para desarrollar, actualizar y revisar las políticas, esta documentado? cada cuanto y bajo que circunstancia se revisan y actualiza la Política? Rpta. TI: Se ampara en las obligaciones contractuales del profesional contratista del área,		60	Conforme lo observado se recomienda revisar y de considerarse pertinente ajustar el documento teniendo en cuenta las bases indicadas por MINTIC en la ***Guía No.2. Elaboración de la política general de seguridad y privacidad de la información***, asegurando la incorporación de los requistios señalados en el campo EVIDENCIA
AD.1.2	Responsable de SI	Revisión y evaluación	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	A.5.1.2	componente planificación					40	
RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN											
A2	**Responsable de SI**	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles**	**A.6**						77	
AD.2.1	**Responsable de SI**	**Organización Interna**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización**	**A.6.1**	**Componente planificación y modelo de madurez gestionado**					84	
AD.2.1.1	Responsable de SI	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	A.6.1.1	Componente planificación	ID.AM-6 ID.GV-2 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5 DE.DP-1 RS.CO-1	Para revisarlo frente a la NIST (Instituto Nacional de Estándares y Tecnología) verifique si 1) los roles y responsabilidades frente a la ciberseguridad han sido establecidos 2) los roles y responsabilidades de seguridad de la información han sido coordinados y alineados con los roles internos y las terceras partes externas 3) Los a) proveedores, b) clientes, c) socios, d) funcionarios, e) usuarios privilegiados, f) directores y gerentes (mandos senior), g) personal de seguridad física, h) personal de seguridad de la información entienden sus roles y responsabilidades, i) Están claros los roles y responsabilidades para la detección de incidentes Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección. Revise la estructura del SGSI: 1) Tiene el SGSI suficiente apoyo de la alta dirección?, esto se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes. 2) Están claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas?, 3) Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección) 4)Están definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales? 5) Están definidos y documentados los niveles de autorización? 6) Se cuenta con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo campañas de sensibilización en seguridad de la información)	NIST 1. No se evidencia 2. No se evidencia 3. No se evidencia Resolución 011 de 2019, por el cual se crea y reglamenta el Comité Operativo Integral de la FUGA 1. Durante la vigencia 2019 se evidencia la realización de un comité de Seguridad de la Información uno ordinario y extraordinario en diciembre 2. No se evidencia 3. No se evidencia 4. No se evidencia para la vigencia 2020 5. No se evidencia 6. De acuerdo a informe de Ejecución del Presupuesto de Gastos e Inversiones, se observa que se tiene el siguiente presupuesto para la vigencia 2020: Gastos de Funcionamiento: 3-1-2-02-02-03-002: Servicios de suministro de infraestructura de hosting y de tecnología de la Información (TI): $6,000,000 3-1-2-02-02-03-006: Servicios de mantenimiento y reparación de computadoras y equipo periférico: $10,000,000 Gastos de Inversión: Vinculados proyectos 7032		20	De acuerdo a lo observado en el campo EVIDENCIAS y teniendo en cuenta que la implementación del Modelo corresponde a una gestión institucional que involucra de manera transversal a varios procesos de la entidad; se recomienda desde la Alta Dirección definir los roles y responsabilidades conforme los temas que deben considerarse en el MSPI (Referencia Hoja *Areas Involucradas* del presente instrumento) De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en la ***Guia No.4. Roles y Responsabilidades***
AD.2.1.2	Responsable de SI	Separación de deberes / tareas	Los deberes y áreas de responsabilidad en conflicto se debe separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	A.6.1.2		PR.AC-4 PR.DS-5 RS.CO-3	Indague como evitan que una persona pueda acceder, modificar o usar activos sin autorización ni detección. La mejor práctica dicta que el inicio de un evento deber estar separado de su autorización. Al diseñar los controles se debería considerar la posibilidad de confabulación. **Tenga en cuenta que para las organizaciones pequeñas la separación de deberes puede ser difícil de lograr, en estos casos se deben considerar controles compensatorios como revisión periódica de, los rastros de auditoria y la supervisión de cargos superiores.**	Documento Política de Seguridad de la Información - Claves de Acceso En la política se establecen controles en los ítem 3. MANEJO Y SEGURIDAD DE INFORMACION EN MEDIOS EXTRAIBLES y 4. SEGURIDAD EN LOS SERVIDORES Y SISTEMAS DE INFORMACIÓN Se evidencia que en el PETIC se establece como debilidad: "La información tiene riesgo de pérdida por el acceso no restringido de los usuarios a los equipos de computo" (Numeral 10. Diagnostico, literal a. Evaluación Interna, acápite ii. Debilidades)		100	
AD.2.1.3	Responsable de SI	Contacto con las autoridades.	Las organizaciones deben tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debe contactar a las autoridades (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de reglamentación y las autoridades de supervisión), y cómo se debe reportar de una manera oportuna los incidentes de seguridad de la información identificados (por ejemplo, si se sospecha una violación de la ley).	A.6.1.3		RS.CO-2	Solicite los procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debería contactar a las autoridades, verifique si de acuerdo a estos procedimientos se han reportado eventos o incidentes de SI de forma consistente.	Se evidencia a través del procedimiento Gestión de Incidentes, Amenazas y Debilidades de Seguridad: 3. Dar respuesta ante incidentes, amenazas y debilidades de seguridad Detectar las causas del problema y los elementos afectados, se debe informar a la Dirección sobre el plan de solución, tiempos involucrados y recursos necesarios, dependiendo del grado de complejidad y magnitud del problema, quien deberá realizar las gestiones correspondientes, incluyendo la comunicación al COLCERT con apoyo técnico del proceso de Gestión tecnológica. De acuerdo lo indicado por el proceso es a través de COLCERT que se establecen los protocolos de Contacto con las autoridades		100	
AD.2.1.4	Responsable de SI	Contacto con grupos de interés especiales	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. Por ejemplo a través de una membresía	A.6.1.4		ID.RA-2	Pregunte sobre las membrecías en grupos o foros de interés especial en seguridad de la información en los que se encuentran inscritos las personas responsables de la SI.	Se tiene acceso a los grupos de WhatsApp SEGURINFO con Alta TIC y con el equipo Distrital TIC, con TER hace referencia a los lideres de tecnología de todas las entidades publicas (DAFP)		100	
AD.2.1.5	Responsable de SI	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza, por ejemplo, un proyecto para un proceso del negocio principal, TI, gestión	A.6.1.5		PR.IP-2	Pregunte como la Entidad integra la seguridad de la información en el ciclo de vida de los proyectos para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Tenga en cuenta que esto no solamente aplica para proyectos de TI, por ejemplo puede aplicar en proyectos de traslado de activos de información, gestión de instalaciones, personal en outsourcing que soporta procesos de la organización. Las mejores prácticas sugieren: a) Que los objetivos de la seguridad de la información se incluyan en los objetivos del proyecto; b) Que la valoración de los riesgos de seguridad de la información se lleve a cabo en una etapa temprana del	Se evidencia a través de PETI, con la formulación de los proyectos del cuatrenio donde se identifica el riesgo de no llevar a cabo el proyecto de cada uno de ellos y en los estudios previos para su ejecución se incorpora la matriz de riesgos previsibles. El seguimiento se lleva a cabo a través de la ejecución de los proyectos		100	
AD.2.2	Responsable de SI	**Dispositivos Móviles y Teletrabajo**	**Garantizar la seguridad del teletrabajo y uso de dispositivos móviles**	**A.6.2**	**Modelo de Madurez Gestionado**					70	
AD.2.2.1	Responsable de SI	Política para dispositivos móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	A.6.2.1			Pregunte si la entidad asigna dispositivos móviles a sus funcionarios o permite que los dispositivos de estos ingresen a la entidad. Revise si existe una política y controles para su uso, que protejan la información almacenada o procesada en estos dispositivos y el acceso a servicios te TI desde los mismos. De acuerdo a las mejores prácticas esta política debe considerar, teniendo en cuenta el uso que se le dé al dispositivo, lo siguiente: a) el registro de los dispositivos móviles; b) los requisitos de la protección física; c) las restricciones para la instalación de software; d) los requisitos para las versiones de software de dispositivos móviles y para aplicar parches; e) la restricción de la conexión a servicios de información; f) los controles de acceso; g) técnicas criptográficas; h) protección contra software malicioso; i) des habilitación remota, borrado o cierre; j) copias de respaldo; k) uso de servicios y aplicaciones web. Cuando la política de dispositivos móviles permite el uso de dispositivos móviles de propiedad personal, la política y las medidas de seguridad relacionadas también deben considerar:	Se evidencia a través del documento Políticas de Seguridad de la Información (GT-PO-01) Versión 2 en el ítem 3. MANEJO Y SEGURIDAD DE INFORMACIÓN EN MEDIOS EXTRAIBLES y 3.5. Manejo equipos de visitantes, Adicionalmente se evidencia a través de la Políticas web tratamiento de datos de manera general el cumplimiento de los siguientes criterios: a) el registro de los dispositivos móviles: queda registrada dentro del programa que hace la configuración de todos los routers (consola de administración de los dispositivos wifi) b) los requisitos de la protección física: Red FUGA_CORP y otra independiente para los invitados (visitantes) d) los requisitos para las versiones de software de dispositivos móviles y para aplicar parches; Se restringe acceso e) la restricción de la conexión a servicios de información; f) los controles de acceso; g) técnicas criptográficas; h) protección contra software malicioso; i) des habilitación remota, borrado o cierre; Se lleva a cabo de manera automatizada con un cronometro k) uso de servicios y aplicaciones web.		100	
AD.2.2.2	Responsable de TICs	Teletrabajo	Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	A.6.2.2		PR.AC-3	Definición de teletrabajo: El teletrabajo hace referencia a todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual". Indague con la entidad si el personal o terceros pueden realizar actividades de teletrabajo, si la respuesta es positiva solicite la política que indica las condiciones y restricciones para el uso del teletrabajo. Las mejores prácticas consideran los siguientes controles: a) la seguridad física existente en el sitio del teletrabajo b) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se tendrá acceso y que pasará a través del enlace de comunicación y la sensibilidad del sistema interno; c) el suministro de acceso al escritorio virtual, que impide el procesamiento y almacenamiento de información en equipo de propiedad privada; d) la amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo equipo, por ejemplo, familia y amigos;	En la entidad si se llevan a cabo actividades de teletrabajo y trabajo en casa, sin embargo no se evidencia como se documenta dentro del documento Políticas de Seguridad de la Información (GT-PO-01) Versión 2		40	Documentar la gestión realizada por la entidad en aras de proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo o trabajo en casa. Conforme la situación actual, evaluar las recomendaciones sobre Ciberseguridad generadas por MINTIC (https://www.teletrabajo.gov.co/622/w3-article-126328.html) e implementar lineamientos que permita asegurar la menor exposición de la entidad a la perdida de información o manipulación de la misma.
SEGURIDAD DE LOS RECURSOS HUMANOS											
AD.3	**Responsable de SI/Gestión Humana/Líderes de los procesos**	**SEGURIDAD DE LOS RECURSOS HUMANOS**		**A.7**						51	
AD.3.1	**Responsable de SI**	**Antes de asumir el empleo**	**Asegurar que el personal y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que son considerados.**	**A.7.1**	**Modelo de Madurez Definido**					80	
AD.3.1.1	Gestión Humana	Selección e investigación de antecedentes	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	A.7.1.1		PR.DS-5 PR.IP-11	Revise el proceso de selección de los funcionarios y contratistas, verifique que se lleva a cabo una revisión de: a) Referencias satisfactorias b) Verificación de la de la hoja de vida del solicitante incluyendo certificaciones académicas y laborales; c) Confirmación de las calificaciones académicas y profesionales declaradas; d) Una verificación más detallada, como la de la información crediticia o de antecedentes penales. Cuando un individuo es contratado para un rol de seguridad de la información específico, las organizaciones deberían asegurar que el candidato tenga la competencia necesaria para desempeñar el rol de seguridad; e) sea confiable para desempeñar el rol, especialmente si es crítico para la organización. f) Cuando un trabajo, ya sea una asignación o una promoción, implique que la persona tenga acceso a las instalaciones de procesamiento de información, y en particular, si ahí se maneja información confidencial, por	Si bien se evidencia que la entidad cuenta con el procedimiento Gestión del Talento Humano (GTH-PD-05) Versión 3 y el formato Lista de Chequeo de Documentos Requeridos para nombramiento y Posesión de Funcionarios (GTH-FT-95) Versión 2, través del cual se solicitan y verifican si los nuevos funcionarios aportan la documentación requerida en el proceso de vinculación. No obstante no se establecen lineamientos respecto a la verificación de los criterios establecidos en este item		80	Establecer o documentar los lineamientos de verificación de la revisión realizada por la entidad a la información suministrada por los funcionarios en el proceso previo a la vinculación laboral, especialmente cuando éste no se lleve a cabo a través de procesos de convotaria realizados por el CNSC
AD.3.1.2	Gestión Humana	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	A.7.1.2		PR.DS-5		**Funcionarios:** De la verificación aleatoria realizada a través de ORFEO de las hojas de vida de los funcionarios vinculados con carácter provisional en el periodo auditado se evidencia el establecimiento dentro del acto administrativo de nombramiento, de una clausula en la cual se indica: "Para desempeñar el cargo se deberán consultar las diferentes políticas, adoptadas por la Fundación Gilberto Álzate Avendaño, así como las funciones del empleo ..." En los nombramientos de libre nombramiento y remoción no se identifica de manera clara como se cumple con lo aquí establecido en la vigencia 2020; para la vigencia 2019 se observa acta de la jornada de inducción en la cual se hace referencia a las políticas de seguridad de la información **Contratistas:** De la verificación realizada de manera aleatoria a contratos de prestación de servicios se observa que en la CLÁUSULA SEXTA - OBLIGACIONES GENERALES DEL CONTRATISTA se establece la siguiente obligación: 3. Guardar reserva con respecto de la información que llegase a conocer con ocasión de la ejecución del contrato, al igual que no compartir ningún tipo de información que repose en los computadores de la entidad con ningún propósito.		80	Documentar como y donde se establecen los acuerdos contractuales con empleados y contratistas, donde se incluyan las responsabilidades y las de la organización en cuanto a la seguridad de la información.
AD.3.2	**Responsable de SI/Líderes de los procesos**	**Durante la ejecución del empleo**	**Asegurar que los funcionarios y contratistas tomen consciencia de sus responsabilidades sobre la seguridad de la información y las cumplan.**	**A.7.1.2**	**Modelo de Madurez Definido**					33	
AD.3.2.1	Responsable de SI	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	A.7.2.1		ID.GV-2	De acuerdo a la NIST los contratistas deben estar coordinados y alineados con los roles y responsabilidades de seguridad de la información. Indague y solicite evidencia del como la dirección se asegura de que los empleados y contratistas: a) Estén debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales. b) Se les suministren las directrices que establecen las expectativas de seguridad de la información de sus roles dentro de la Entidad. c) Logren un nivel de toma de conciencia sobre seguridad de la información pertinente a sus roles y responsabilidades dentro de la organización y estén motivados para cumplir con las políticas. d) Tengan continuamente las habilidades y calificaciones apropiadas y reciban capacitación en forma regular.	a. De la verificación realizada de manera aleatoria a contratos de prestación de servicios se observa que en la CLÁUSULA SEXTA - OBLIGACIONES GENERALES DEL CONTRATISTA se establece la siguiente obligación: 3. Guardar reserva con respecto de la información que llegase a conocer con ocasión de la ejecución del contrato, al igual que no compartir ningún tipo de información que repose en los computadores de la entidad con ningún propósito. b. a e. no se identifica de manera clara como se da cumplimiento		40	Establecer el protocolo o lineamiento a través del cual se exijar a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
AD.3.2.2	Responsable de SI/Líderes de los procesos	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	A.7.2.2	Componente planeación Modelo de Madurez Inicial	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	Entreviste a los líderes de los procesos y pregúnteles que saben sobre la seguridad de la información, cuales son sus responsabilidades y como aplican la seguridad de la información en su diario trabajo. Pregunte como se asegura que los funcionarios, Directores, Gerentes y contratistas tomen conciencia en seguridad de la información, alineado con las responsabilidades, políticas y procedimientos existentes en la Entidad. Solicite el documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección. Verifique que se han tenido en cuenta buenas prácticas como: a) Desarrollar campañas, elaborar folletos y boletines. b) Los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la	Para la vigencia 2019 se desarrollo a nivel de Comité Directivo en la sesión de Diciembre y en el 2020 se programo dentro de la ejecución del PIC		60	Fortalecer las estrategias de divulgación de seguridad de la información a todos los niveles institucionales y documentar la gestión realizada, con el fin de garantizar el cumplimiento de cada uno de los requisitos del criterio evaluado. De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en la ***Guia No. 14. Plan de Comunicaciones, sensibilización y comunicación de seguridad de la información***
AD.3.2.3	Responsable de SI	Proceso disciplinario	Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la	A.7.2.3			Pregunte cual es el proceso disciplinario que se sigue cuando se verifica que ha ocurrido una violación a la seguridad de la información, quien y como se determina la sanción al infractor?	No se evidencia como se da cumplimiento a este criterio por parte de la Oficina de Control Disciplinario		0	Establecer el procedimiento o documentar como se da cumplimiento del criterio evaluado
AD.3.3	**Responsable de SI**	**Terminación y cambio de empleo**	**Proteger los intereses de la Entidad como parte del proceso de cambio o terminación de empleo.**	**A.7.3**	**Modelo de Madurez Definido**					40	
AD.5.1.3	Responsable de SI	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	A.7.3.1		PR.DS-5 PR.IP-11	Revisar los acuerdos de confidencialidad, verificando que deben acordar que después de terminada la relación laboral o contrato seguirán vigentes por un periodo de tiempo.	A través del clausulado de los Contratos se establece la obligación de cumplir por parte de los contratistas los acuerdos de confidencialidad, amparados con la clausula de INCUMPLIMIENTO. Para los funcionarios se da través del obligaciones como servidores públicos		40	Establecer el procedimiento o documentar como se da cumplimiento del criterio evaluado
GESTIÓN DE ACTIVOS											
AD.4	**Responsable de SI**	**GESTIÓN DE ACTIVOS**		**A.8**						69	
AD.4.1	**Responsable de SI**	**Responsabilidad de los activos**	**Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.**	**A.8.1**	**Modelo de Madurez Gestionado**					90	
AD.4.1.1	Responsable de SI	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	A.8.1.1	Componente Planificación Modelo de madurez inicial	ID AM-1 ID AM-2 ID.AM-5	Solicite el inventario de activos de información, revisado y aprobado por la alta Dirección y revise: 1) Ultima vez que se actualizó 2) Que señale bajo algún criterio la importancia del activo 3) Que señale el propietario del activo Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión. De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos. **Tenga en cuenta para la calificación:** 1) Si Se identifican en forma general los activos de información de la Entidad, están en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, están en 60. 3) Si se revisa y monitorean periódicamente los activos de información de la entidad, están en 80.	De conformidad con la información publicada en la página web de la entidad, link de transparencia (https://www.fuga.gov.co/transparencia/activos-informacion) se observa que la entidad tiene publicado el documento Activos Información: Software, hardware y servicios 1. El documento publicado aparece con fecha de actualización Diciembre de 2019 2. Se establece la criticidad del activo de información para las operaciones internas y para el servicio (Bajo, Medio y Alto) 3. Se indica la localización del activo y quien es su custodio No obstante se evidencia que la información registrada no se encuentra actualizada (Número de CPU difiere con lo reportado en Derechos de Autor) La información la actualiza el Profesional Contratista TI.		60	Fortalecer los controles de tal manera que la información relacionada con el inventario de activos Software, hardware y servicios de encuentre actualizada. De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC: ***Guia No.2. Elaboración de la política general de seguridad y privacidad de la información*** ***Guia No 5 Gestión Clasificación de Activos***
AD.4.1.2	Responsable de SI	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	A.8.1.2		ID AM-1 ID AM-2	Solicite el procedimiento para asegurar la asignación oportuna de la propiedad de los activos. Tenga en cuenta que la propiedad se debería asignar cuando los activos se crean o cuando son entregados a la Entidad. De acuerdo a las mejores prácticas el propietario de los activos (individuo o entidad, que es responsable por el activo) tiene las siguientes responsabilidades: a) asegurarse de que los activos están inventariados; b) asegurarse de que los activos están clasificados y protegidos apropiadamente; c) definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables; d) asegurarse del manejo apropiado del activo cuando es eliminado o destruido.	De acuerdo a lo observado en los documentos publicados en la intranet, se observa que el procedimiento con el que se asegura la asignación de los activos es el de Manejo y Control de bienes (RF-PD-01) Versión 7 y el Instructivo Toma Física de Inventarios (RF-IN-01) Versión 2		100	
AD.4.1.3	Responsable de SI	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	A.8.1.3			Pregunte por la política, procedimiento, directriz o lineamiento que defina el uso aceptable de los activos, verifique que es conocida por los empleados y usuarios de partes externas que usan activos de la Entidad o tienen acceso a ellos.	Se evidencia a través de: 1. Política de Seguridad de la Información (GT-PO-01) Versión 2. Numeral 3. Manejo y Seguridad de Información en medios Extraíbles, 4. Seguridad en los servidores y sistemas de información 2. Guía Metodológica de gestión de activos de Información (GT-GU-01) Versión 2 Las acciones de mejora se evidencian a través de las actividades propuestas para la vigencia 2020 en marco del resultado de la verificación realizada por la OCI a Derechos de Autor La divulgación de la actualización de los documentos se llevó a cabo a través de correo electrónico de fecha 26/02/2020		100	
AD.4.1.4	Responsable de SI	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	A.8.1.4		PR.IP-11	Revisar las políticas , normas , procedimientos y directrices relativas a los controles de seguridad de la información durante la terminación de la relación laboral por ejemplo, la devolución de los activos de información (equipos, llaves, documentos , datos, sistemas) , las llaves físicas y de cifrado, la eliminación de los derechos de acceso, etc. En caso de que un funcionario o tercero sea el dueño del activo indague como se asegura la transferencia de la información a la Entidad y el borrado seguro de la información de la Entidad. En caso en que un empleado o usuario de una parte externa posea conocimientos que son importantes para las operaciones regulares, esa información se debería documentar y transferir a la Entidad. Durante el periodo de notificación de la terminación, la Entidad debería controlar el copiado no autorizado de la información pertinente (por ejemplo, la propiedad intelectual) por parte de los empleados o contratistas que han finalizado el empleo.	Si bien se evidencia que a través de los siguientes documentos se establecen de manera general controles: 1. Política de Seguridad de la Información (GT-PO-01) Versión 2. Numeral 5. Administración de Usuarios 2. Clausula Sexta - Obligaciones Generales del Contratista: Numeral 8. Responder por la custodia y buen manejo de los equipos y elementos suministrados por la Fundación para el cumplimiento de sus obligaciones, de tal manera que sean devueltos en buen estado, una vez terminado el contrato, de acuerdo con el procedimiento establecido para el manejo y control de bienes de la entidad. 3. Guía Metodológica de gestión de Activos de Información (GT-GU-01) Versión 2. establece en sus políticas de operación lo siguiente: "Los funcionarios deberán devolver los activos asignados al terminar su contrato laboral" A través del Formato de Paz y Salvo se verifica la devolución de los activos tanto para los contratistas como de los funcionarios		100	
AD.4.2	**Responsable de SI**	**Clasificación de información**	**Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.**	**A.8.2**						67	
AD.4.2.1	Responsable de SI	Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	A.8.2.1	Modelo de Madurez Inicial		Solicite el procedimiento mediante el cual se clasifican los activos de información y evalúe: 1) Que las convenciones y criterios de clasificación sean claros y estén documentados 2) Que se defina cada cuanto debe revisarse la clasificación de un activo 3) La clasificación debería valorarse analizando la confidencialidad, integridad y disponibilidad. Solicite muestras de inventarios de activos de información clasificados y evalúe que se aplican las políticas y procedimientos de clasificación definidos. Evalúe si los procesos seleccionados aplican de manera consistente estas políticas y procedimientos.	Se observa dentro de los documentos SIG del proceso, la Guía metodológica de gestión de activos de información (GT-GU-01) Versión 2, sin embargo este documento no establece de manera clara los criterios evaluados. De la verificación realizada al Formato activos de información (GT-FT-10) Versión 1 se observa que se establecen convenciones respecto a la criticidad para las operaciones internas y para el servicio, no obstante no se hace aclaración de los criterios para cada convención, no se define la periodicidad de revisión de la clasificación y los criterios para valorar la confidencialidad, integridad y disponibilidad Por último también se observa que en el documento Políticas de Seguridad de la Información (GT-PO-01) Versión 2, si bien incluye el numeral 2. CLASIFICACION Y CONTROL DE ACTIVOS, no se observa que estos lineamientos estén articulados con los criterios evaluados		60	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en la ***Guia No 5 Gestión Clasificación de Activos***
AD.4.2.2	Responsable de SI	Etiquetado de la información		A.8.2.2		PR.DS-5 PR.PT-2	Solicite el procedimiento para el etiquetado de la información y evalúe: 1) Aplica a activos en formatos físicos y electrónicos (etiquetas físicas, metadatos) 2) Que refleje el esquema de clasificación establecido 3) Que las etiquetas se puedan reconocer fácilmente 4) Que los empleados y contratistas conocen el procedimiento de etiquetado Revise en una muestra de activos el correcto etiquetado	Si bien se hace referencia al etiquetado de la información en los documentos Políticas internas de Seguridad y tratamiento de datos. 6.2.1. Archivo de documentos y Manual recomendaciones de seguridad para funcionarios y contratistas de la FUGA, y en las tablas de MEDIDAS DE SEGURIDAD identificadas en el Ítem 6.3.7 Consolidado Medidas de Seguridad, no se identifica el cumplimiento de los requisitos aqui identificados		60	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en la ***Guia No 5 Gestión Clasificación de Activos***
AD.4.2.3	Responsable de SI	Manejo de activos		A.8.2.3		PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-5 PR.IP-6 PR.PT-2	Solicite los procedimientos para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación. De acuerdo a las mejores prácticas evidencie si se han considerado los siguientes asuntos: a) Restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación; b) Registro formal de los receptores autorizados de los activos; c) Protección de copias de información temporal o permanente a un nivel coherente con la protección de la información original; d) Almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes; e) Marcado claro de todas las copias de medios para la atención del receptor autorizado. f) De acuerdo a NIST la información almacenada (at rest) y en tránsito debe ser protegida.	Se evidencian directrices generales relacionadas con los criterios evaluados en el documento Manual Institucional de Gestión Documental del Proceso de Patrimonio Institucional y con la implementación de la TRD del proceso NO obstante no es clara como se aplica el criterio **d** de lo establecido		80	Incluir el requisito "Almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes" en el documento a través del cual se incorporan los temas vinculados a este criterio
AD.4.3	**Responsable de TICs**	**Manejo de medios**	**Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios.**	**A.8.3**						50	
AD.4.3.1	Responsable de TICs	Gestión de medios removibles		A.8.3.1		PR.DS-3 PR.IP-6 PR.PT-2	Solicite las directrices, guías, lineamientos y procedimientos para la gestión de medios removibles, que consideren: a) Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debe remover de forma que no sea recuperable; b) cuando resulte necesario y práctico, se debe solicitar autorización para retirar los medios de la organización, y se debe llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría; d) si la confidencialidad o integridad de los datos se consideran importantes, se deben usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles; f) se deben guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida casuales de los datos; h) sólo se deben habilitar unidades de medios removibles si hay una razón de valida asociada a los procesos la Entidad para hacerlo; i) En donde hay necesidad de usar medios removibles, se debería hacer seguimiento a la transferencia de información a estos medios (Por ejemplo DLP)	En Procedimiento Manejo y Control de Bienes se establece los lineamientos para dar de baja los activos, incluidos los activos de información (Software y Hardware) a través del concepto técnico del profesional del área de TI En el procedimiento Gestión de Soluciones y Gestión de Tecnología, actividad 6 y 7 relaciona las acciones para retirar del servicio algún bien No obstante no es claro como se da cumplimiento a lo establecido en los requisitos d,f y h		40	Documentar las directrices o lineamientos que la entidad considera pertinentes que permitan garantizar: d) si la confidencialidad o integridad de los datos se consideran importantes, se deben usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles; f) se deben guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida casuales de los datos; h) sólo se deben habilitar unidades de medios removibles si hay una razón de valida asociada a los procesos la Entidad para hacerlo;
AD.4.3.2	Responsable de TICs	Disposición de los medios		A.8.3.2		PR.DS-3 PR.IP-6	Solicite los procedimientos existentes para garantizar que los medios a desechar o donar, no contienen información confidencial que pueda ser consultada y copiada por personas no autorizadas. Verifique si se ha realizado esta actividad y si existen registros de la misma.	Si bien en el desarrollo del seguimiento a Derechos de Autor Software se indico por parte del proceso que: "Se procede con la destrucción del original y de todas sus copias, incluidas las licencias que acreditan su propiedad. En el acta de destrucción se deja constancia de la extinción total del software, En caso de un bien intangible a nivel de software se procede a la desinstalación en los equipos, si se tiene conocimiento que puede ser usado en otro Ente y Entidad, previa autorización del fabricante o siempre y cuando no existan restricciones, se procede a realizar el traslado mediante acta de entrega; la transacción implica el retiro definitivo del mismo, cabe resaltar que para cualquiera de los dos casos esta actividad debe ir sujeta a un acto administrativo" Sin embargo no se evidencia el procedimiento que establece estos lineamientos		60	Documentar las directrices o lineamientos que la entidad considera pertinentes que permitan garantizar el cumplimiento del criterio evaluado.
AD.4.3.3	Responsable de TICs	Transferencia de medios físicos		A.8.3.3		PR.DS-3 PR.PT-2	Solicite las directrices definidas para la protección de medios que contienen información durante el transporte. Verifique de acuerdo a las mejores prácticas que se contemple:	No aplica		n/a	
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO											
AD.5	**Responsable de la Continuidad**	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		**A.17**						26,5	
AD.5.1	**Responsable de la Continuidad**	**Continuidad de la seguridad de la información**	**La continuidad de la seguridad de la información debe incluir en los sistemas de gestión de la continuidad del negocio de la Entidad.**	**A.17.1**						13	
AD.5.1.1	Responsable de la Continuidad	Planificación de la continuidad de la seguridad de la información		A.17.1.1	Modelo de Madurez Gestionado	ID.BE-5 PR.IP-9	Indagar si la Entidad cuenta con un BCP (Bussines Continuity Plan) o DRP (Disaster Recovery Plan). Determine si aplica para procesos críticos solamente o se han incluido otros procesos o por lo menos se ha reconocido la necesidad de ampliarlo a otros procesos (para determinar el nivel de madurez) Evalúe si se ha incluido en estos planes y procedimientos los requisitos de seguridad de la información. Tenga en cuenta que en ausencia de una planificación formal de continuidad de negocio y recuperación de desastres, la dirección de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones operacionales normales. Como alternativa, una organización puede llevar a cabo un análisis de impacto en el negocio de los aspectos de seguridad de la información, para determinar los requisitos de seguridad de la información aplicables a situaciones adversas. De acuerdo a la NIST también se deben tener planes de respuesta a incidentes y recuperación de incidentes. **Tenga en cuenta para la calificación:**	Si bien se evidencia el procedimiento Gestión de Incidentes, Amenazas y Debilidades de Seguridad (GT-PD-03) Versión 1, a través del cual se "Establecer las directrices ante la ocurrencia de incidentes o la detección de amenazas y/o debilidades que pudiesen comprometer la seguridad de los activos de información con el fin de detener un protocolo especifico para responder ante cualquier requerimiento que afecte la disponibilidad de los servicios tecnológicos que se presenten al interior de la entidad basándose en la mejores practicas documentadas por MSPI emitido por los entes de control." no se identifica los criterios establecidos en este aparte		20	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en: ***Guia No 3 Procediimiento de seguridad de la Información*** ***Guia No 10 Continuidad del negocio***

AD.5.1.2	Responsable de la Continuidad	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa,	A.17.1.2	Modelo de Madurez Definido	ID.BE-5 PR.IP-4 PR.IP-9 PR.IP-9	Verifique si la entidad cuenta con a) Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias. b) Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información. c) Planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección. Revise si los controles de seguridad de la información que se han implementado continúan operando durante un evento contingente. Si los controles de seguridad no están en capacidad de seguir brindando seguridad a la información, se la Entidad debe establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.	a. La estructura se define en el PETI y se implemento en la contingencia de cuarentena vigencia 2020, a través de los lineamientos impartidos directamente por la directora y Subdirectora de Gestión Corporativa para atender la situación. b. Se evidencia a través de las funciones de establecidas en el manual de funciones y las obligaciones contractuales de los profesionales de apoyo de TI c. No se evidencia		20	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en: ***Guia No 3 Procediimento de seguridad de la Información*** ***Guia No 10 Continuidad del negocio***
AD.5.1.3	Responsable de la Continuidad	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		A.17.1.3	Modelo de Madurez Optimizado	PR.IP-4 PR.IP-10	Indague y solicite evidencias de la realización de pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información; Tenga en cuenta que la verificación de los controles de continuidad de la seguridad de la información es diferente de las pruebas y verificación generales de seguridad de la información. Si es posible, es preferible integrar la verificación de los controles de continuidad de negocio de seguridad de la información con las pruebas de recuperación de desastres y de continuidad de negocio de la organización.	No se evidencia		0	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en: ***Guia No 3 Procediimento de seguridad de la Información*** ***Guia No 10 Continuidad del negocio***
AD.5.2	**Responsable de la Continuidad**	**Redundancias**	**Asegurar la disponibilidad de las instalaciones de procesamiento de la información.**	**A.17.2**						**40**	
AD.5.2.1	Responsable de la Continuidad	Disponiblilidad de instalaciones de procesamiento de información		A.17.2.1		ID.BE-5	Verifique si la Entidad cuenta con arquitecturas redundantes, ya sea un centro de cómputo principal y otro alterno o componentes redundantes en el único centro de cómputo. Indague como se han definido las necesidades de los procesos para seleccionar que elementos deben ser redundantes. Solicite si aplica las pruebas aplicadas para asegurar que un componente redundante funciona de la forma prevista durante una emergencia o falla.	Se tienen dos data center uno en casa amarilla y otra en la sede principal, se ubica los sistemas de información en cualquier de los data center de conformidad con la necesidad, no obstante no se tienen redundancias a nivel de los servidores.		40	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos
CUMPLIMIENTO											
AD.6	**Responsable de SI/Responsable de TICs/Control Interno**	**CUMPLIMIENTO**		**A.18**						**88,5**	
AD.6.1	**Responsable de SI**	**Cumplimiento de requisitos legales y contractuales**	**Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.**	**A.18.1**		**ID.GV-3**	**De acuerdo a la NIST: Los requerimientos legales y regulatorios respecto de la ciberseguridad, incluyendo la privacidad y las libertades y obligaciones civiles, son entendidos y gestionados.**			**90**	
AD.6.1.1	Responsable de SI	Identificación de la legislación aplicable y de los requisitos contractuales.		A.18.1.1	**Modelo de Madurez Gestionado Cuantitativamente**		Solicite la relación de requisitos legales, reglamentarios, estatutarios, que le aplican a la Entidad (Normograma). Indague si existe un responsable de identificarlos y se definen los responsables para su cumplimiento.	De acuerdo a lo observado en la página web de la entidad, link de transparencia (https://www.fuga.gov.co/transparencia/normograma) se evidencia que la entidad tiene la relación de requisitos legales, reglamentarios, estatutarios que le aplica (Normograma). El formato establecido Matriz de Cumplimiento Legal (CEM-FT-16) Versión 1, establece el proceso, responsable y área o dependencia que le aplica Se observa que la ultima actualización publicada corresponde a Septiembre de 2019		100	
AD.6.1.2	Responsable de TICs	Derechos de propiedad intelectual.		A.18.1.2			1) Solicite los procedimientos para el cumplimiento de los requisitos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. 2) Verifique si la Entidad cuenta con una política publicada sobre el cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos. Esta política debe estar orientada no solo al software, si no también a documentos gráficos, libros, etc. 3) Indague como se controla que no se instale software ilegal. 4) Indague si se tiene un inventario de software instalado y se compara con el número de licencias adquiridas para asegurar que no se incumplen los derechos de propiedad intelectual. Tenga en cuenta los controles que deben existir para asegurar que no se exceda ningún número máximo de usuarios permitido dentro de la licencia.	De acuerdo a lo observado en el seguimiento realizado al cumplimiento de Derechos de Autor se identificaron los siguientes documentos: • Guía Metodológica de gestión de activos de información (Código GT-GU-01 Versión 2). 8. POLÍTICAS PARA EL USO ACEPTABLE DE LOS ACTIVOS: Usos no autorizados: Está prohibido realizar cambios a los activos informáticos de la Fundación Gilberto Álzate, sin contar con la autorización formal del responsable de las áreas o del proceso en el que esté el activo Informático", "No debe cambiar ni alterar de ninguna forma el hardware o el software de los sistemas de información de la Fundación Gilberto Álzate" y "Los funcionarios deben cumplir con los derechos de autor y los contratos de licencia" • Políticas de Seguridad de la Información (GTI-POL-01) Versión 1 del 13/02/2017. 8. MANEJO DE ACCESO A INTERNET – "Queda prohibida la descarga que no cumpla con la normatividad vigente de copyright y similar". No obstante lo anterior, no se evidencia en los procedimientos vigentes, la operatividad de la politica asi como los controles que permitan dar cumplimiento a la misma Ver informe cumplimiento Derechos de Autor 2019		80	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos
AD.6.1.3	Responsable de SI	Protección de registros.	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales	A.18.1.3		PR.IP-4	Revise si la Entidad cuenta con tablas de retención documental que especifiquen los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción. Posibles tipos de registros pueden ser registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales, los medios de almacenamiento permitidos pueden ser papel, microfichas, medios magnéticos, medios ópticos etc.	De acuerdo a la información publicada en la entidad a través de la página web y la intranet (https://www.fuga.gov.co/transparencia/tablas-retencion-documental), se evidencia el documento Tablas de Retención Documental , en el cual se identifica el tipo de registros y el periodo de retención y Disposición final. La destrucción a nivel de sistemas de información se documenta a través del procedimiento de Manejo y Control de Bines, no obstante no se evidencia clarea la identificación del almacenamiento, manejo y destrucción de los mismos.		80	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos
AD.6.1.4	Responsable de SI	Protección de los datos y privacidad de la información relacionada con los datos personales.	Se deben asegurar la protección y privacidad de la información personal tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.	A.18.1.4		DE.DP-2	Indague sobre las disposiciones que ha definido la Entidad para cumplir con la legislación de privacidad de los datos personales, ley estatutaria 1581 de 2012 y decreto 1377 que reglamenta la ley de 2013. 1) Revise si existe una política para cumplir con la ley 2) Si están definidos los responsables 3) Si se tienen identificados los repositorios de datos personales 4) Si se ha solicitado consentimiento al titular para tratar los datos personales y se guarda registro de este hecho. 5) Si se adoptan las medidas técnicas necesarias para proteger las bases de datos donde reposan estos datos.	De conformidad con la información publicada en la página web de la entidad, link de transparencia (https://www.fuga.gov.co/transparencia/politicas-seguridad) se observa que la entidad referencia como Politicas de seguridad de la información del sitio web y protección de datos personales, las siguientes politicas, manual y protocolo: * Politicas de Seguridad de la Información: El documento publicado no se encuentra actualizado. * Política de tratamiento de la información y protección de datos personales * Politicas internas de Seguridad y tratamiento de datos * Politicas web tratamiento de datos * Manual recomendaciones de seguridad * Protocolo de atención a titulares información De acuerdo a lo indicado por los profesionales del proceso, la gestión de identificación de repositorios se encuentra reportada a la Superintendencia de Industria y Comercio SIC a través del Registro Nacional de Bases de Datos (RNBD), el cual incluye entre otros ORFEO, Talento Humano, Gestión Jurídica, Bronx y Comunicaciones (Se aporta correo electrónico con los reportes) El consentimiento de los titulares se registro a través de formulario implementado por la Subdirección de Gestión Artística y Cultural en el cual los ciudadanos manifestaban su voluntad de uso de su información. Talento Humano (SIDEAP). Jurídica (SECOP), ORFEO (Protocolo de Creación de Terceros), Comunicaciones En el caso de los Amigos de la Fuga se tiene en el drive respaldado con gsuit, ORFEO a nivel de bakcup, las otras bases (comunicaciones, talento humano) respaldado con el servidor y juridica con el bakcup		100	
AD.6.1.5	n/a	Reglamentación de controles criptográficos.		A.18.1.5			n/a				
AD.6.2	**Control interno**	**Revisiones de seguridad de la información**		**A.18.2**	**Modelo de Madurez Gestionado Cuantitativamente**					**87**	
AD.6.2.1	Control interno	Revisión independiente de la seguridad de la información		A.18.2.1			Investigue la forma como se realizan revisiones independientes (por personas diferentes o no vinculadas a un proceso o área que se revisa), de la conveniencia, la adecuación y la eficacia continuas de la gestionar la seguridad de la información. Para esto solicite: 1) El plan de auditorías del año 2017 2) El resultado de las auditorías del año 2017 3) Las oportunidades de mejora o cambios en la seguridad de la información identificados.	Verificados los Planes de Auditoria de las vigencias 2019 no se evidencia la incorporación de actividades y ejecución de revisiones independientes No obstante se observa que en el 2020 se incluyo la Auditoria Gestión de Tecnologia que incluye el componente del MSPI		60	
AD.6.2.2	Control interno	Cumplimiento con las políticas y normas de seguridad.	Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.	A.18.2.2		PR.IP-12	1) Verifique si los gerentes aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento de las políticas y estándares de seguridad. 2) Verifique la revisión periódica del cumplimiento del centro de cómputo con las políticas y normas de seguridad establecidas. 3) Verifique si los sistemas de información son revisados regularmente para asegurar el cumplimiento de las normas de seguridad de la información	De acuerdo a lo informado por el proceso se gestionan estos criterios: 1. A nivel de dirección, subdirecciones y jefes de oficina se da cumplimiento de las políticas a través de los formatos establecidos dentro de los procedimientos del proceso y los criterios definidos dentro de las politicas 2. Se gestiona a través del plan de mantenimiento: a nivel lógico a través de los ingenieros del área, a nivel físico a través del operador contratado y los controles definidos dentro de la politicas (Acceso restringido, copias de seguridad y demás directrices) 3. Se lleva a cabo a través de la ejecución de los contratos de los ingenieros del área.		100	
AD.6.2.3	Responsable de SI	Revisión de cumplimiento técnico.	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.	A.18.2.3		ID.RA-1	Verifique si se realizan evaluaciones de seguridad técnicas por o bajo la supervisión de personal autorizado, apoyado en herramientas automáticas o con revisiones manuales realizadas por especialistas. Solicite evidencia de las últimas pruebas realizadas, sus resultados y seguimiento para asegurar que las brechas de seguridad fueron solucionadas.	Se hace a nivel de firewall (virus, ataques de negación de servicio), se hace la estructuración de la licencia (contrato) A nivel de malware		100	
RELACIONES CON LOS PROVEEDORES											
AD.7	**Responsable de compras y adquisiciones**	**RELACIONES CON LOS PROVEEDORES**		**A.15**						**90**	
AD.7.1	Responsable de compras y adquisiciones	Seguridad de la información en las relaciones con los proveedores	Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores	A.15.1	Modelo de Madurez Definido		1) Solicite la política de seguridad de la información para las relaciones con los proveedores, que indique los requisitos de SI para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización, esta política debe reflejarse en los acuerdos con los proveedores que deben estar documentados. 2) Verifique en la muestra de proveedores con acceso a los activos de información (no necesariamente son proveedores de tecnología de la información, por ejemplo pueden ser proveedores que tengan por ejemplo un proceso de nomina en outsourcing), se hayan suscrito acuerdos (ANS) formales donde se establezcan y acuerden todos los requisitos de seguridad de la información pertinentes con cada proveedor. 3) Verifique para los proveedores si se tiene en cuenta los riesgos de SI asociados a la cadena de suministro, por ejemplo para los proveedores en la nube es muy común que se apoyen en otros proveedores para	1. A nivel contractual en las obligaciones se establece niveles de confidencialidad, en los estudios previos se identifica con la matriz de riesgos previsibles. Si bien en las Políticas internas de Seguridad y tratamiento de datos se hace referencia a las relaciones con los proveedores respecto al manejo de datos, no se identifica de manera clara el cumplimiento del criterio evaluado. 2. Contratos (Soporte Lógico y Mediacommerce) 3. Contrato de hosting (Group): el que permite el uso de la página web e intranet		80	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en la ***Guia No 3 Procedimientos de Seguridad de la Información.***
AD.7.2	Responsable de compras y adquisiciones	Gestión de la prestación de servicios de proveedores	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores	A.15.2	Modelo de Madurez Definido		1) Indague y solicite evidencia en una muestra de proveedores seleccionada, como la entidad hace seguimiento, revisa y audita con regularidad de acuerdo a la política la prestación de servicios de los proveedores y el cumplimiento de los compromisos respecto a la seguridad de la información. 2) Indague y evidencie como se gestionan los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, los incidentes de seguridad de la información y la revaloración de los riesgos. 2)	De acuerdo a lo informado por los ingenieros del proceso se indica: 1. A través de la ejecución de los contratos de los proveedores; cuando los servicios son tercerizados, se hace especificamente con el de hosting, conectividad (enlaces de conectividad). La verificaciones se hace a través de el acceso a un usuario de la consola de monitoreo para validar la saturación de los canales. Cuando es de mantenimiento se hace acompañamiento in situ. 2. Se gestiona con la evaluación monitoreo y control de los riesgos previsibles y documentándolo en los seguimientos. A través de la gestión de la mesa de ayuda la cual registra los casos para dar soporte por parte de los ingenieros vinculados al proceso.		100	

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

FUNDACIÓN GILBERTO ALZATE AVENDAÑO

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
CONTROL DE ACCESO											
T.1	**Responsable de SI/Responsable de TICs**	**CONTROL DE ACCESO**		**A.9**	**Componente planificación y modelo de madurez nivel gestionado**					**75**	
T.1.1	Responsable de SI	**REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO**	**Se debe limitar el acceso a información y a instalaciones de procesamiento de información.**	**A.9.1**	Modelo de madurez definido					**50**	
T.1.1.1	Responsable de SI	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	A.9.1.1		PR.DS-5	Revisar que la política contenga lo siguiente: a) los requisitos de seguridad para las aplicaciones del negocio; b) las políticas para la divulgación y autorización de la información, y los niveles de seguridad de la información y de clasificación de la información; c) la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes; d) la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios; e) la gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles;	Se hace referecia al control de acceso en los documentos: Políticas internas de Seguridad y tratamiento de datos Procedimiento Gestión de Incidentes, Amenazas y Debilidades de Seguridad No obstante los mismos no identifcan de manera clara el cuplimiento de los requisitos evaluados		40	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en la ***Guia No 2 Elaboración de la política general de seguridad y privacidad de la información***
T.1.1.2	Responsable de TICs	Acceso a redes y a servicios en red	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	A.9.1.2		PR.AC-4 PR.DS-5 PR.PT-3	Revisar la política relacionada con el uso de redes y de servicios de red y verificar que incluya: a) las redes y servicios de red a los que se permite el acceso; b) los procedimientos de autorización para determinar a quién se permite el acceso a qué redes y servicios de red; c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y a los servicios de red; d) los medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas); e) los requisitos de autenticación de usuarios para acceder a diversos servicios de red; f) el seguimiento del uso de servicios de red.	En el documento Políticas de Seguridad de la Información (GT-PO-01) Versión 2, se identifica el item 8. MANEJO DE ACCESO A INTERNET, y el procedimiento Seguridad de redes, hace refencia al acceso a las redes, no obstante no se identifica de manera clara el cumplimiento de los criterios a, b y f De acuerdo a lo informado por el proceso en la aplicación de la lista de verificación se indica que la entidad no tiene una red robusta que requiera la aplicabilidad de todos los criterios establecidos; se tiene el tema de la VPN, seguimiento a los servicios, autorización y autenticación.		60	Documentar como se da cumplimiento a los requisitos establecidos para este criterio e identificarlos dentro de la política establecida.
T.1.2	Responsable de SI	**GESTIÓN DE ACCESO DE USUARIOS**	**Se debe asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.**	**A.9.2**	Modelo de madurez gestionado cuantitativamente					**83**	
T.1.2.1	Responsable de SI	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	A.9.2.1		PR.AC-1	Revisar el proceso para la gestión y la identificación de los usuarios que incluya: a) Identificaciones únicas para los usuarios, que les permita estar vinculados a sus acciones y mantener la responsabilidad por ellas; el uso de identificaciones compartidas solo se debe permitir cuando sea necesario por razones operativas o del negocio, y se aprueban y documentan; b) deshabilitar o retirar inmediatamente las identificaciones de los usuarios que han dejado la organización; c) identificar y eliminar o deshabilitar periódicamente las identificaciones de usuario redundantes; d) asegurar que las identificaciones de usuario redundantes no se asignen a otros usuarios.	En el documento Políticas de Seguridad de la Información (GT-PO-01) Versión 2, se identifica: 1. Item 7. SEGURIDAD DE LA CONTRASEÑA y Item 9. CLAVES DE ACCESO Los usuarios redudantes se controlan a través de validaciones frente al controlador de dominio lo que asegura que no se creen usuarios con el mismo nombre ya creado para otro perfil.		100	
T.1.2.2	Responsable de SI	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	A.9.2.2		PR.AC-1	Revisar el proceso para asignar o revocar los derechos de acceso otorgados a las identificaciones de usuario que incluya: a) obtener la autorización del propietario del sistema de información o del servicio para el uso del sistema de información o servicio; b) verificar que el nivel de acceso otorgado es apropiado a las políticas de acceso y es coherente con otros requisitos, tales como separación de deberes; c) asegurar que los derechos de acceso no estén activados antes de que los procedimientos de autorización estén completos; d) mantener un registro central de los derechos de acceso suministrados a una identificación de usuario para acceder a sistemas de información y servicios; e) adaptar los derechos de acceso de usuarios que han cambiado de roles o de empleo, y retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han dejado la organización; f) revisar periódicamente los derechos de acceso con los propietarios de los sistemas de información o servicios.	Se basa en el tema de ingreso y retiro de los empleados, se verifica en el tema de los riesgos se hace una validación aleatoria de los ingresos y egresos. El control que se hace es operativo y se basa en el procedimiento de Gestión del Talento Humano . El controlador del dominio da el acceso a la red y a los sistema de información, al deshabilitar el usuario se impide el acceso tanto a la red como a los sistemas sincronizados. Se encuentran documentados de manera general en el Procedimiento Asignación de cuentas.		80	Revisar las directices establecidas y fortalecerlas de tal manera que se asegure el cumplimiento de los requisitos aquí establecidos.
T.1.2.3	Responsable de SI	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	A.9.2.3		PR.AC-4 PR.DS-5	Revisar la asignación de derechos de acceso privilegiado a través de un proceso de autorización formal de acuerdo con la política de control de acceso pertinente. el proceso debe incluir los siguientes pasos: a) Identificar los derechos de acceso privilegiado asociados con cada sistema o proceso, (sistema operativo, sistema de gestión de bases de datos, y cada aplicación) y los usuarios a los que es necesario asignar; b) definir o establecer los derechos de acceso privilegiado a usuarios con base en la necesidad de uso y caso por caso, alineada	Los usuarios privilegiados se tratan de la misma manera que los usuarios regulares de negocio, a través de los lineamientos establecidos en el Procedimiento Asignación de cuentas.		80	Revisar las directices establecidas y fortalecerlas de tal manera que se asegure el cumplimiento de los requisitos aquí establecidos.
T.1.2.4	Responsable de SI	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	A.9.2.4		PR.AC-1	Revisar el proceso, que incluya: a) establecer la firma de una declaración para mantener confidencial la información de autenticación secreta personal, y mantener la información de autenticación secreta del grupo (cuando es compartida) únicamente dentro de los miembros del grupo; esta declaración firmada se puede incluir en los términos y condiciones del empleo para todos los que los usuarios ; b) estipular que todos los usuarios deben mantener su propia información de autenticación secreta, y se les suministra una autentificación secreta temporal segura, que se obligue a cambiar al usarla por primera vez; c) establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle la nueva información de autenticación secreta de reemplazo o temporal;	Se evidencia a través de la Politica de Seguridad de la Información en el ítem 7. SEGURIDAD DE LA CONTRASEÑA. El numeral f se lleva a cabo a través correo electrónico donde se da al usuario las indicaciones sin embargo no se evidencia de manera clara el acuse de recibido		80	Revisar las directices establecidas y fortalecerlas de tal manera que se asegure el cumplimiento de los requisitos aquí establecidos.
T.1.2.5	Responsable de SI	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	A.9.2.5			Revisar los derechos de acceso que incluya: a) examinar los derechos de acceso de los usuarios periódicamente y después de cualquier cambio, promoción, cambio a un cargo a un nivel inferior, o terminación del empleo; b) establecer que los derechos de acceso de usuario se revisan y reasignan cuando pasan de un rol a otro dentro de la misma organización; c) definir las autorizaciones para los derechos de acceso privilegiado y revisar periódicamente; d) verificar las asignaciones de privilegios periódicamente, para asegurar que no se hayan obtenido privilegios no autorizados; e) revisar y registrar los cambios a las cuentas privilegiadas periódicamente.	Se basa en el tema de ingreso y retiro de los empleados, se verifica en el tema de los riesgos se hace una validación aleatoria de los ingresos y egresos. El control que se hace es operativo y se basa en el procedimiento de Gestión del Talento Humano . El controlador del dominio da el acceso a la red y a los sistema de información, al deshabilitar el usuario se impide el acceso tanto a la red como a los sistemas sincronizados. Se encuentran documentados de manera general en el Procedimiento Asignación de cuentas.		80	Revisar las directices establecidas y fortalecerlas de tal manera que se asegure el cumplimiento de los requisitos aquí establecidos.
T.1.2.6	Responsable de SI	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	A.9.2.6			Revisar los derechos de acceso a la información y a los activos asociados con instalaciones de procesamiento de información, antes de que el empleo termine o cambie, dependiendo de la evaluación de factores de riesgo que incluya: a) terminación o cambio lo inicia el empleado, el usuario de la parte externa o la dirección, y la razón de la terminación; b) revisar las responsabilidades actuales del empleado, el usuario de la parte externa o cualquier otro usuario; c) verificar el valor de los activos accesibles en la actualidad.	Se basa en el tema de ingreso y retiro de los empleados, se verifica en el tema de los riesgos se hace una validación aleatoria de los ingresos y egresos. El control que se hace es operativo y se basa en el procedimiento de Gestión del Talento Humano . El controlador del dominio da el acceso a la red y a los sistema de información, al deshabilitar el usuario se impide el acceso tanto a la red como a los sistemas sincronizados. Se encuentran documentados de manera general en el Procedimiento Asignación de cuentas.		80	Revisar las directices establecidas y fortalecerlas de tal manera que se asegure el cumplimiento de los requisitos aquí establecidos.
T.1.3	**Responsable de SI**	**RESPONSABILIDADES DE LOS USUARIOS**	**Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.**	**A.9.3**	Modelo de madurez definido					**80**	
T.1.3.1	Responsable de SI	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación	A.9.3.1		PR.AC-1	Revisar si el proceso de notificación a usuarios incluye: a) Mantener la confidencialidad de la información de autenticación secreta, asegurándose de que no sea divulgada a ninguna otra parte, incluidas las personas con autoridad; b) evitar llevar un registro (en papel, en un archivo de software o en un dispositivo portátil) de autenticación secreta, a menos que	Se evidencia a través de la Politica de Seguridad de la Información en el ítem 7. SEGURIDAD DE LA CONTRASEÑA.		80	Se recomienda fortalecer tips de divulgación relacionados con los aspectos de los numerales 1, 2, 3 y g
T.1.4	Responsable de SI	**CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**	**Se debe evitar el acceso no autorizado a sistemas y aplicaciones.**	**A.9.4**	Modelo de madurez gestionado cuantitativamente					**87**	
T.1.4.1	Responsable de SI	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	A.9.4.1		PR.AC-4 PR.DS-5	Revisar las restricciones de acceso a través de la aplicación individual del negocio y de acuerdo con la política de control de acceso definida; que incluya: a) suministrar menús para controlar el acceso a las funciones de sistemas de aplicaciones; b) controlar a qué datos puede tener acceso un usuario particular; c) controlar los derechos de acceso de los usuarios, (a leer, escribir, borrar y ejecutar); d) controlar los derechos de acceso de otras aplicaciones; e) limitar la información contenida en los elementos de salida; f) proveer controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos.	Se identifica el control de acceso a través del procedimiento Asignación de cuentas y la validación de los perfiles y roles en la solicitud de creación de usuarios requerida por los jefes de oficina o responsables de los procesos. No obstante no se evidencia de manera clara lo relacionado con el numeral a de los criterios evaluados.		80	Revisar las directices establecidas y fortalecerlas de tal manera que se asegure el cumplimiento de los requisitos aquí establecidos.
T.1.4.2	Responsable de SI	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	A.9.4.2		PR.AC-1	Revisar el procedimiento de ingreso que incluya: a) no visualizar los identificadores del sistema o de la aplicación sino hasta que el proceso de ingreso se haya completado exitosamente; b) visualizar una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador; c) evitar los mensajes de ayuda durante el procedimiento de ingreso, que ayudarían a un usuario no autorizado; d) validar la información de ingreso solamente al completar todos los datos de entrada. ante una condición de error, el sistema	De acuerdo a lo indicado en la aplicación de la lista de verifiación, este criterio no aplica para la entidad, por que es suficiente la política, no se requiere un procedimiento de acceso segurio por que no se tienen transacciones propias, las que se realizan corresponden a seguridad bancaria y a la de la SDH		n/a	
T.1.4.3	Responsable de TICs	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	A.9.4.3		PR.AC-1	Revisar el sistema de gestión de contraseñas que incluya: a) cumplir el uso de identificaciones y contraseñas de usuarios individuales para mantener la rendición de cuentas; b) permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluyan un procedimiento de confirmación para permitir los errores de entrada; c) Exigir por que se escojan contraseñas de calidad; d) Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez; e) Exigir por que se cambien las contraseñas en forma regular, según sea necesario: f) llevar un registro de las contraseñas usadas previamente, e impedir su reusó; g) no visualizar contraseñas en la pantalla cuando se está ingresando; h) almacenar los archivos de las contraseñas separadamente de los datos del sistema de aplicaciones; i) almacenar y transmitir las contraseñas en forma protegida.	En el documento Políticas de Seguridad de la Información (GT-PO-01) Versión 2, se identifica: 1. Item 7. SEGURIDAD DE LA CONTRASEÑA y Item 9. CLAVES DE ACCESO Los controles se llevan a cabo a través del Controlador de Dominio De acuerdo a lo indicado por el proceso en la matriz del instrumento diligencia en el autodiagnostico: Existe una politica de contraseña de usuario de administrador segura y otra de usuario estandar que esadministrada por el servidor de dominio con caraceterisitcas de robustez		100	
T.1.4.4	Responsable de TICs	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	A.9.4.4		PR.AC-2	Revisar las directrices para el uso de programas utilitarios con la capacidad de anular los controles de sistemas y de aplicaciones, que incluyan. a) utilizar procedimientos de identificación, autenticación y autorización para los programas utilitarios; b) separar los programas utilitarios del software de aplicaciones; c) limitar el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados;	De acuerdo a lo informado en la aplicación de la lista de verificación, los programas utilitarios en la entidad se han venido desinstalando por obsolecencia, por lo cual no aplica el criterio evaluado		n/a	
T.1.4.5	Responsable de TICs	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	A.9.4.5		PR.AC-3	Revisar el procedimiento para la gestión de códigos fuente de los programas, que incluya: a) definir en donde sea posible, las librerías de fuentes de programas no se deben mantener en los sistemas operativos; b) gestionar los códigos fuente de los programas y las librerías de las fuentes de los programas se debería hacer de acuerdo con procedimientos establecidos; c) establecer que el personal de soporte deben tener acceso restringido a las librerías de las fuentes de los programas; d) definir que la actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores sólo se deben hacer una vez que se haya recibido autorización apropiada; e) establecer que los listados de programas se deben mantener en un entorno seguro; f) conservar un registro de auditoría de todos los accesos a la librerías de fuentes de programas; g) mantener y copiar las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios.	En el procedimiento Implementación de soluciones y servicios de Tecnología se vinculan los formatos de CheckList y Paso a Producción en los cuales se evidencia que la gestión de los códigos fuente son de uso exclusivo del personal operativo del personal de sistemas, validado con el procevimiento acceso cuentas. (Acceso a librerias y códigos fuente) No obstante no se evidencia de manera clara la implementación de los controles que garanticen el cumplimiento del control e		80	Revisar las directices establecidas y fortalecerlas de tal manera que se asegure el cumplimiento de los requisitos aquí establecidos.
CRIPTOGRAFÍA											
T.2	**Responsable de SI**	**CRIPTOGRAFÍA**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles**	**A.10**						**20**	
T.2.1	**Responsable de SI**	**CONTROLES CRIPTOGRÁFICOS**	**Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.**	**A.10.1**	Modelo de madurez gestionado cuantitativamente					**20**	
T.2.1.1	Responsable de SI	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	A.10.1.1			Revisar la política sobre el uso de la criptográfica, que incluya: a) establecer el enfoque de la dirección con relación al uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se deben proteger la información del negocio; b) realizar una valoración de riesgos, que identifique el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido. c) utilizar la encriptación para la protección de información transportada por dispositivos de encriptación móviles o removibles, o a través de líneas de comunicación; d) gestionar las llaves y los métodos para la protección de llaves criptográficas y la recuperación de información encriptada, en el	De acuerdo a lo indicado en la aplicación de la lista de verificación, a nivel criptografico se han implementado acciones a nivel de las redes wifi y a través de las contraseñas emitidas por el controlador de dominio, no obstante se aclara que este uso no aplica para la entidad por cuanto no se tienen el uso de transacciones internas propias de manejo de recursos o de información de alta confidencialidad		20	Teniendo en cuenta que el criterio busca asegurar la *"confidencialidad y autenticidad de la información que circula o se genera a través de los diferentes sistemas de información"* se recomienda establecer directrices o lineamientos que permitan implementar controles efectivos relacionados con este tema
T.2.1.2	Responsable de SI	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo	A.10.1.2			Revisar el sistema de gestión de llaves que debe estar basado en un grupo establecido de normas, procedimientos y métodos seguros para: a) generar llaves para diferentes sistemas criptográficos y diferentes aplicaciones; b) generar y obtener certificados de llaves públicas;	No aplica conforme lo indicado en el ítem anterior.		n/a	
SEGURIDAD FÍSICA Y DEL ENTORNO											
T.3	**Responsable de la seguridad física/Responsable de SI/Líderes de los procesos**	**SEGURIDAD FÍSICA Y DEL ENTORNO**		**A.11**						65	
T.3.1	**Responsable de la seguridad física**	**ÁREAS SEGURAS**	**Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.**	**A.11.1**	Modelo de madurez definido					**60**	
T.3.1.1	Responsable de la seguridad física	Perímetro de seguridad física	Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	A.11.1.1		PR.AC-2	Revisar las directrices relacionadas con los perímetros de seguridad física: a) definir los perímetros de seguridad, y el emplazamiento y fortaleza de cada uno de los perímetros deben depender de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de una valoración de riesgos; b) establecer los perímetros de una edificación o sitio que contenga instalaciones de procesamiento de la información debe ser físicamente seguros; el techo exterior, las paredes y el material de los pisos del sitio deben ser de construcción sólida, y todas las paredes externas deben estar protegidas adecuadamente contra acceso no autorizado con mecanismos de control (barras, alarmas, cerraduras); las puertas y ventanas deben estar cerradas con llave cuando no hay supervisión, y se debe considerar	En el documento Políticas de Seguridad de la Información (GT-PO-01) Versión 2, se identifica: 1. Item 10. SEGURIDAD FISICA No obstante no se identifica de manera clara el cumplimiento de los criterios e, f y g		40	Evaluar de manera articulada con Gestión de Recursos Físicos la implementación de las acciones que permitan garantizar el cumplimiento de los criterios pendientes de gestionar
T.3.1.2	Responsable de SI	Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	A.11.1.2		PR.AC-2 PR.MA-1	Revisar los controles de acceso físico y las siguientes directrices: a) tener un registro de la fecha y hora de entrada y salida de los visitantes, y todos los visitantes deben ser supervisados a menos que su acceso haya sido aprobado previamente; solo se les debe otorgar acceso para propósitos específicos autorizados y se deben emitir instrucciones sobre los requisitos de seguridad del área y de los propósitos de emergencia. La identidad de los visitantes se deben autenticar por los medios apropiados; b) establecer que el acceso a las áreas en las que se procesa o almacena información confidencial se debería restringir a los individuos autorizados solamente mediante la implementación de controles de acceso apropiados, (mediante la implementación	De acuerdo a lo indicado en la aplicación de la lista de verificación y la matriz de autodiagnostico: Estan definidos y protegidos los lugares como los Datacenter de la entidad donde solo puede ingresar a traves de biometrico. La empresa de vigilancia lleva un control del personal de visitantes y las bitacoras son revisadas por la subdirección gestión corporativa		100	Si bien se da cumplimiento, teniendo en cuenta la ubicación física actual del área de Tecnología, se recomienda evaluar la separación de ésta de tal manera que pueda garantizarse de manera integral el control de acceso físico a las instalaciones de procesamiento de información.
T.3.1.3	Líderes de los procesos	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	A.11.1.3			Revisar las siguientes directrices relacionadas con la seguridad a oficinas, recintos e instalaciones: a) establecer que las instalaciones clave deben estar ubicadas de manera que se impida el acceso del público; b) definir donde sea aplicable, las edificaciones deben ser discretas y dar un indicio mínimo de su propósito, sin señales obvias externas o internas, que identifiquen la presencia de actividades de procesamiento de información; c) establecer que las instalaciones deben estar configuradas para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también se debe ser el apropiado; d) definir los directorios y guías telefónicas internas que identifican los lugares de las instalaciones de procesamiento de información confidencial no deben ser accesibles a ninguna persona no autorizada.	En el documento Políticas de Seguridad de la Información (GT-PO-01) Versión 2, se identifica: 1. Item 10. SEGURIDAD FISICA No obstante se precisa que los criterios establecidos, de acuerdo a la infraestructura fisica de la entidad, no aplica de manera detallada como lo indica los requerimientos		n/a	
T.3.1.4	Responsable de SI	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	A.11.1.4		ID.BE-5 PR.AC-2 PR.IP-5	De acuerdo a la NIST deben identificarse los elementos de resiliencia para soportar la entrega de los servicios críticos de la entidad.	De acuedo a lo indicado en la aplicación de la lista de verificación, se tiene identificada la necesidad pero aún esta en proceso la asignación de recursos. Se tiene virtualizado el correo electrónico y los sistemas de información Humano y Contar, lo que garantiza que en un evento a nivel interno sigan operando los servicios, lo recursos corresponde a la protección de la información del servidor a nivel de archivos, de lo cual no hay un respaldo fuera de la entidad.		40	Articular con SGST y ARL la implementación de las acciones que permitan garantizar el cumplimiento de los criterios pendientes de gestionar a nivel de protección fisica
T.3.1.5	Responsable de SI	Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	A.11.1.5	Componente planeación		Revisar trabajo en área segura y las siguientes directrices: a) establecer que el personal solo debe conocer de la existencia de un área segura o de actividades dentro de un área segura, con base en lo que necesita conocer; b) definir que el trabajo no supervisado en áreas seguras se debe evitar tanto por razones de seguridad como para evitar oportunidades para actividades malintencionadas;	N.A		n/a	
T.3.1.6	Responsable de la seguridad física	Áreas de despacho y carga	Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	A.11.1.6		PR.AC-2	Revisar las siguientes directrices: a) establecer que el acceso al área de despacho y de carga desde el exterior de la edificación se debería restringir al personal identificado y autorizado; b) definir que el área de despacho y carga se debe diseñar de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras partes de la edificación; c) establecer que las puertas externas de un área de despacho y carga se aseguran cuando las puertas internas están abiertas; d) definir que el material que ingresa se inspecciona y examina para determinar la presencia de explosivos, químicos u otros materiales peligrosos, antes de que se retiren del área de despacho y carga; e) establecer que el material que ingresa se registra de acuerdo con los procedimientos de gestión de activos al entrar al sitio; f) definir que los despachos entrantes y salientes se están separados físicamente, en donde sea posible; g) establecer que el material entrante se inspecciona para determinar evidencia de manipulación durante el viaje. Si se descubre esta manipulación, se debería reportar de inmediato al personal de seguridad.	N.A		n/a	
T.3.2	**Responsable de SI**	**EQUIPOS**	**Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.**	**A.11.2**	Modelo de madurez definido					**69**	
T.3.2.1	Responsable de SI	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	A.11.2.1		PR.IP-5	Revisar las siguientes directrices para proteger los equipos: a) establecer que los equipos están ubicados de manera que se minimice el acceso innecesario a las áreas de trabajo; b) definir que las instalaciones de procesamiento de la información que manejan datos sensibles están ubicadas cuidadosamente para reducir el riesgo de que personas no autorizadas puedan ver la información durante su uso; c) establecer que las instalaciones de almacenamiento se aseguran para evitar el acceso no autorizado; d) definir que los elementos que requieren protección especial se salvaguardan para reducir el nivel general de protección	Se evidencia a través del procedimiento Plan de mantenimiento Infraestructura Tecnológica. No obstante no es claro como se da cumplimiento a los criterios d, f, g, h, i		80	De forma conjunta con SGST y Recursos Fisicos establecer los lineamientos que consideren pertinentes de tal manera que se incorporen los requisitos relacionados con infraestructura del criterio evaluado.
T.3.2.2	Responsable de TICs	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	A.11.2.2		ID.BE-4 PR.IP-5	Revisar los servicios de suministro (electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) para que cumplan: a) cumplir con las especificaciones de los fabricantes de equipos y con los requisitos legales locales; b) evaluar regularmente en cuanto a su capacidad para estar al ritmo del crecimiento e interacciones del negocio con otros servicios de soporte; c) inspeccionar y probar regularmente para asegurar su funcionamiento apropiado; d) si es necesario, contar con alarmas para detectar mal funcionamiento; e) si es necesario, tener múltiples alimentaciones con diverso enrutado físico.	Se protege a través de la UPS (Sede Grifos: Telecomunicaciones y algunos equipos por un periodo aproximadamente de 5 mint), en esta sede en particular se presenta el inconveniente que los contadores no se encuentran ubicados en la propia sede sino en la casa contingua, por lo cual el acceso a estos depende de un tercero. La protección es completa para la Sede Principal y la Casa Amarilla que permite un espacio de tiempo para un correcto apagado de servidores de 20 y 40 minutos dependiendo la carga		80	Evaluar, a través del proceso de Gestión de Recursos Físicos la pertinencia de gestionar el traslado de los contadores de energía de la sede Grifos de tal manera que haya independencia y control sobre el suministro de energia a los equipos de esa sede
T.3.2.3	Responsable de TICs	Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información deben estar protegido contra interceptación, interferencia o daño.	A.11.2.3		ID.BE-4 PR.AC-2 PR.IP-5	Revisar las siguientes directrices para seguridad del cableado: a) establecer que las líneas de potencia y de telecomunicaciones que entran a instalaciones de procesamiento de información deben ser subterráneas en donde sea posible, o deben contar con una protección alternativa adecuada; b) establecer que los cables de potencia están separados de los cables de comunicaciones para evitar interferencia; c) definir para sistemas sensibles o críticos los controles adicionales que se deben considerar incluyen: 1) la instalación de conduit apantallado y recintos o cajas con llave en los puntos de inspección y de terminación; 2) el uso de blindaje electromagnético para proteger los cables; 3) el inicio de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se conectan a los cables	De acuerdo a lo indicado en la aplicación de la lista de verificación, se lleva a cabo la siguiente gestión: La estructuración de la canaleta que es la que permite la protección fisica del cableado. Los puntos de inspección del rack de comunicaciones ubicado en la sede principal, esta protegido y guardado. El de Grifos falta ponerle la llave. La sede Grigos no esta adaptado totalmente para el funcionamiento de oficinas, se adecuo de manera alteranativa El inicio de barridos técnicos se hace a través de inspecciones visuales de manera aleatoria. Se verifica con un comando PIN los tráficos que tiene la red, si estan saturados se hace la revisión visual.		80	Documentar las directrices o lineamientos que garanticen el cumplimiento de los requisitos a evaluar en este criterio
T.3.2.4	Responsable de TICs	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	A.11.2.4		PR.MA-1 PR.MA-2	Revisar las siguientes directrices para mantenimiento de equipos: a) mantener los equipos de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor; b) establecer que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos; c) llevar registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo; d) implementar los controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si éste lo lleva a cabo el personal en el sitio o personal externo a la organización; en donde sea necesario, la información confidencial se debe borrar del equipo, o el personal de mantenimiento debería retirarse (cleared) lo suficientemente de la información; e) cumplir todos los requisitos de mantenimiento impuestos por las políticas de seguros; f) establecer que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.	De conformidad con la verificación realizada a los documentos SIG del proceso de observan: 1. Procedimiento Gestión de soluciones y servicios de tecnología -Mesa de ayuda (GT-PD-02) Versión 2 2. Procedimiento Gestión de soluciones y servicios de tecnologías y MTO. (GT-PD-03) Version 1 3. Procedimiento Respaldo de la información (GT-PD-05) Versión 1 Respecto al literal de se evidencia a través de los informes de ejecución de los contratos suscritos para llevar a cabo el plan de mantenimiento No obstante no se identifica e manera clara el cumplimiento del criterios e		80	Documentar las directrices o lineamientos que garanticen el cumplimiento del requisito relacinado con las políticas de seguros
T.3.2.5	Responsable de TICs	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	A.11.2.5		PR.MA-1	Revisar las siguientes directrices para el retiro de activos: a) identificar a los empleados y usuarios de partes externas que tienen autoridad para permitir el retiro de activos del sitio; b) establecer los límites de tiempo para el retiro de activos y verificar que se cumplen las devoluciones; c) definir cuando sea necesario y apropiado, registrar los activos se retiran del sitio y cuando se hace su devolución; d) documentar la identidad, el rol y la filiación de cualquiera que maneje o use activos, y devolver esta documentación con el equipo, la información y el software. Información adicional	Se vincula su cumplimiento a traves del proceso de Recursos Físicos, con los formatos de Control de Entrada y Salida de Bienes y el de Salida e Ingreso de Portatiles. No se tiene un protocolo definido para el control del retiro de activos frente a los guardas de seguridad de las sedes de la entidad		80	De manera conjunta con Recursos Fisicos evaluar la pertinencia de establecer una directriz o lineamiento que garantice el cumplimiento de lo normado
T.3.2.6	Responsable de SI	Seguridad de equipos y activos fuera de las instalaciones	Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	A.11.2.6		ID.AM-4	De acuerdo a la NIST se deben catalogar los sistemas de información externos. Revisar las siguientes directrices para proteger los equipos fuera de las instalaciones: a) establecer que los equipos y medios retirados de las instalaciones no se deben dejar sin vigilancia en lugares públicos; b) seguir en todo momento las instrucciones del fabricante para proteger los equipos, (contra exposición a campos electromagnéticos fuertes); c) controlar los lugares fuera de las instalaciones, tales como trabajo en la casa, teletrabajo y sitios temporales se deben	De acuerdo a lo indicado en la matriz de autodiagnostico: Se encuentra los formatos de retiro de equipos de computo. No obstante no se identifica de manera clara como se da cumplimiento a los diferentes criterios aquí evaluados.		40	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos
T.3.2.7	Responsable de TICs	Disposición segura o reutilización de equipos	Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	A.11.2.7		PR.DS-3 PR.IP-6	Revisar las siguientes directrices del proceso de borrado de discos y de encriptación del disco (para evitar la divulgación de la información confidencial cuando se dispone del equipo o se le da un destino diferente, siempre y cuando): a) establecer que el proceso de encriptación sea suficientemente fuerte y abarque todo el disco (incluido el espacio perdido, archivos temporales de intercambio, etc.); b) definir que las llaves de encriptación sean lo suficientemente largas para resistir ataques de fuerza bruta; c) establecer que las llaves de encriptación se mantengan confidenciales.	De acuerdo a lo indicado en la matriz de autodiagnostico: La entidad esta al tanto y se dispondra a realizar las marcaciones. No obstante no se identifica de manera clara como se da cumplimiento a los diferentes criterios aquí evaluados.		20	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos

T.3.2.8	Responsable de SI	Equipos de usuario desatendidos	Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.	A.11.2.8			Revisar que el procedimiento equipos de usuarios desatendidos incluya: a) establecer que se cierren las sesiones activas cuando hayan terminado, a menos que se puedan asegurar mediante un mecanismo de bloqueo apropiado (un protector de pantalla protegido con contraseña); b) establecer que es obligatorio salir de las aplicaciones o servicios de red cuando ya no los necesiten; c) asegurar que los computadores o dispositivos móviles contra uso no autorizado mediante el bloqueo de teclas o un control equivalente (acceso con contraseña, cuando no están en uso).	Se evidencia en el documento Políticas de Seguridad de la Información GT-PO-01 Versión 2. , numerales 5. ADMINISTRACIÓN DE USUARIOS, 6. SEGURIDAD DE LAS CUENTAS DE CORREO ELECTRÓNICO, 9. CLAVES DE ACCESO y 10. SEGURIDAD FISICA Adicionalmente en la aplicación de la lista de verificación se indica que el criterio c se hace a través del controlador de dominio. En la matriz de autodiagnostico se indica: Se realizan campañas de socialización se envia por GPO el bloqueo de equipo tras un tiempo de inactividad. La entidad esta al tanto y se dispondra a realizar las marcaciones		80	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos
T.3.2.9	Responsable de SI	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	A.11.2.9		PR.PT-2	Revisar las siguientes directrices para escritorio limpio: a) establecer que la información sensible o crítica del negocio, (sobre papel o en un medio de almacenamiento electrónico), se guarda bajo llave (idealmente, en una caja fuerte o en un gabinete u otro mueble de seguridad) cuando no se requiera, especialmente cuando la oficina esté desocupada. b) definir un procedimiento para la gestión de equipos desatendidos; los computadores y terminales deben estar fuera del sistema y estar protegidos con un sistema de bloqueo de la pantalla y el teclado, controlado por una contraseña, token o mecanismo similar de autenticación de usuario, y deben estar protegidos por bloqueo de teclas u otros controles, cuando no están en uso; c) evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (escáneres, cámaras digitales); d) establecer que los medios que contienen información sensible o clasificada se deben retirar de las impresoras inmediatamente.	Si bien en el documento Políticas de Seguridad de la Información GT-PO-01 Versión 2. se hace mencion en el numeral 10. SEGURIDAD FISICA, item 10.3 Escritorio Limpio; a. Clasificación de información (Gestión Documental) c y d se controlan con los usuarios de red y de impresora No se evidencia como se da cumplimiento al literal b		80	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos
SEGURIDAD DE LAS OPERACIONES											
T.4	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS OPERACIONES**		**A.12**						58	
T.4.1	**Responsable de TICs**	**PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**	**Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.**	**A.12.1**	Modelo de madurez definido					**30**	
T.4.1.1	Responsable de TICs	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.	A.12.1.1			Revisar los procedimientos de operación con instrucciones operacionales, que incluyen: a) instalar y configurar sistemas; b) establecer el procesamiento y manejo de información, tanto automático como manual; c) establecer la gestión de las copias de respaldo; d) definir los requisitos de programación, incluidas las interdependencias con otros sistemas, los tiempos de finalización del primer y último trabajos; e) establecer las instrucciones para manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución del trabajo, incluidas las restricciones sobre el uso de sistemas utilitarios; f) definir contactos de apoyo y de una instancia superior, incluidos los contactos de soporte externo, en el caso de dificultades operacionales o técnicas inesperadas; g) establecer las instrucciones sobre manejo de medios y elementos de salida, tales como el uso de papelería especial o la gestión de elementos de salida confidenciales, incluidos procedimientos para la disposición segura de elementos de salida de trabajos fallidos; h) definir los procedimientos de reinicio y recuperación del sistema para uso en el caso de falla del sistema;	Se evidencia de manera general procedimientos documentados relacionados con: a Implementación de soluciones y servicios de Tecnología b. No se evidencia claramente c. Respaldos de la Información d. No se evidencia claramente e. Implementación de soluciones y servicios de Tecnología f. No se evidencia claramente g. Manejo y Control de Blenes h. No se evidencia claramente i. No se evidencia claramente j. No se evidencia claramente		40	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos
T.4.1.2	Responsable de TICs	Gestión de cambios	Se debe controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad	A.12.1.2		PR.IP-1 PR.IP-3	Revisar los procedimientos de control de cambios, que incluyen: a) Identificar y registrar los cambios significativos; b) Planificar y puesta a prueba de los cambios; c) Valorar los impactos potenciales, incluidos los impactos de estos cambios en la seguridad de la información; d) Tener un procedimiento de aprobación formal para los cambios propuestos;	No se evidencia		0	A través de las Oficinas Asesora de Planeación y Comunicaciones, gestionar la documentación relacionada con el Control de Cambios, que incluya los criterios establecidos aquí evaluados.
T.4.1.3	Responsable de TICs	Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	A.12.1.3		ID.BE-4	Revisar los procedimientos para la gestión de la demanda de capacidad, que incluyen: a) Eliminar datos obsoletos (espacio en disco); b) realizar cierre definitivo de aplicaciones, sistemas, bases de datos o ambientes; c) optimizar cronogramas y procesos de lotes; d) optimizar las consultas de bases de datos o lógicas de las aplicaciones; e) realizar una negación o restricción de ancho de banda a servicios ávidos de recursos, si estos no son críticos para el negocio	Se adelanto la gestión de documentación a través del Procedimiento Gestión de soluciones y servicios de tecnología y MTO, que hace referencia a datos obsoletos, sin embargo no se identifica de manera clara documentación relacionada con la negación o restricción de ancho de banda		40	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos
T.4.1.4	Responsable de TICs	Separación de los ambientes de desarrollo, pruebas y operación	Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	A.12.1.4		PR.DS-7	Revisar los procedimientos para la separación de ambientes, que incluyen: a) definir y documentar las reglas para la transferencia de software del estatus de desarrollo al de operaciones. b) establecer que el software de desarrollo y de operaciones debe funcionar en diferentes sistemas o procesadores de computador y en diferentes dominios o directorios; c) definir que los cambios en los sistemas operativos y aplicaciones se deben probar en un entorno de pruebas antes de aplicarlos	Si bien se tienen documentados formatos de pasar a producción un sistema de información a través del procedimiento Implementación de soluciones y servicios de Tecnología, no se definen documentalmente los criterios evaluados en este ítem		40	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos
T.4.2	**Responsable de SI**	**PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS**	**Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.**	**A.12.2**						**60**	
T.4.2.1	Responsable de SI	Controles contra códigos maliciosos	Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	A.12.2.1	Modelo de madurez gestionado	PR.DS-6 DE.CM-4 RS.MI-2	Revisar las siguientes directrices: a) establecer una política formal que prohíba el uso de software no autorizado; b) implementar controles para evitar o detectar el uso de software no autorizado (listas blancas de aplicaciones); b) implementar controles para evitar o detectar el uso de sitios web malicioso o que se sospecha que lo son (listas negras); d) establecer una política formal para proteger contra riesgos asociados con la obtención de archivos y de software ya sea mediante redes externas o cualquier otro medio, indicando qué medidas externas se deben tomar; e) reducir las vulnerabilidades de las que pueda aprovecharse el software malicioso, (medio de la gestión de la vulnerabilidad técnica); f) llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos del negocio; se debería investigar formalmente la presencia de archivos no aprobados o de enmiendas no autorizadas; g) instalar y actualizar software de detección y reparación del software malicioso en los computadores y medios como una medida de control, en forma rutinaria; el análisis realizado debería incluir: 1) el análisis de cualquier archivo recibido por la red o por cualquier forma de medio de almacenamiento, para detectar el software malicioso, antes de uso; 2) el análisis de los adjuntos y descargas de los correos electrónicos, para determinación del software malicioso antes de uso; este análisis se debería llevar a cabo en diferentes lugares, (los servidores de los correos electrónicos, en los computadores de escritorio) y cuando se ingresa a la red de la organización; el análisis de páginas web, para determinar el software malicioso; h) definir procedimientos y responsabilidades relacionadas con la protección contra el software malicioso en los sistemas, formación acerca del uso de dichos procedimientos, reporte y recuperación de ataques de software malicioso; i) preparar planes de continuidad del negocio apropiados, para la recuperación de ataques de software malicioso, incluidos todos los datos necesarios, copias de respaldo del software y disposiciones para recuperación; j) implementar procedimientos para recolectar información en forma regular, (la suscripción a listas de correos o la verificación	De acuerdo a lo observado en el seguimiento realizado al cumplimiento de Derechos de Autor se identificaron los siguientes documentos: • Guía Metodológica de gestión de activos de información (Código GT-GU-01 Versión 2). 8. POLÍTICAS PARA EL USO ACEPTABLE DE LOS ACTIVOS: Usos no autorizados: Está prohibido realizar cambios a los activos informáticos de la Fundación Gilberto Álzate, sin contar con la autorización formal del responsable de las áreas o del proceso en el que esté el activo informático", "No debe cambiar ni alterar de ninguna forma el hardware o el software de los sistemas de información de la Fundación Gilberto Álzate" y "Los funcionarios deben cumplir con los derechos de autor y los contratos de licencia" • Políticas de Seguridad de la Información (GTI-POL-01) Versión 1 del 13/02/2017. 8. MANEJO DE ACCESO A INTERNET – "Queda prohibida la descarga que no cumpla con la normatividad vigente de copyright y similar". Si bien de manera general se cumplen los criterios con la experticia del personal vinculado al proceso, no se encuentran documentados. Ver informe cumplimiento Derechos de Autor 2019		60	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos
T.4.3	**Responsable de TICs**	**COPIAS DE RESPALDO**	**Proteger contra la pérdida de datos.**	**A.12.3**	Modelo de madurez gestionado					**60**	
T.4.3.1	Responsable de TICs	Respaldo de la información	Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	A.12.3.1		PR.DS-4 PR.IP-4	Revisar las siguientes directrices: a) producir registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados; b) establecer la cobertura (copias de respaldo completas o diferenciales) y la frecuencia con que se hagan las copias de respaldo debe reflejar los requisitos del negocio de la organización, los requisitos de la seguridad de la información involucrada, y la criticidad de la información para la operación continua de la organización; c) definir las copias de respaldo se debe almacenar en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal;	Se gestiona a través del procedimiento Respaldos de la Información (GT-PD-05) Versión 1, no obstante no se identifica de manera clara como da cumplimiento a los criterios c y f		60	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos
T.4.4	Responsable de SI	**REGISTRO Y SEGUIMIENTO**	**Registrar eventos y generar evidencia.**	**A.12.4**	Modelo de madurez gestionado cuantitativamente					**55**	
T.4.4.1	Responsable de SI	Registro de eventos	Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	A.12.4.1	Modelo de madurez gestionado cuantitativamente	PR.PT-1 DE.CM-3 RS.AN-1	Revisar los registros de eventos que incluyan: a) identificar los usuarios; b) establecer las actividades del sistema; c) definir las fechas, horas y detalles de los eventos clave, (entrada y salida); d) identificar el dispositivo o ubicación, si es posible, e identificador del sistema; e) tener registros de intentos de acceso al sistema exitosos y rechazados; e) definir registros de datos exitosos y rechazados y otros intentos de acceso a recursos; g) establecer los cambios a la configuración del sistema; h) definir el uso de privilegios;	De acuerdo a lo informado en la aplicación de la lista de verificación, se da cumplimiento de maneral con el reporte incidentes y el seguimiento que se hace a la gestión estos, documentados de manera general Gestión de soluciones y servicios de tecnología -mesa de ayuda. Adicionalmente se revisan lo log y es un recursos que ayuda a revisar las fallas		60	Documentar de manera integral en los reportes de incidentes los requisitos establecidos en el criterio
T.4.4.2	Responsable de SI	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	A.12.4.2		PR.PT-1	Revisar los procedimientos y controles dirigidos a proteger contra cambios no autorizados de la información del registro y contra problemas con la instalación de registro, que incluya: a) verificar todas las alteraciones a los tipos de mensaje que se registran; b) establecer los archivos log que son editados o eliminados; c) verificar cuando se excede la capacidad de almacenamiento del medio de archivo log, lo que da como resultado falla en el registro de eventos, o sobre escritura de eventos pasados registrados.	Los registros se valoran a través de ORFEO (Confidencialidad, integralidad, disponibilidad), tambien a través del control de las cuentas (perfiles de los usuarios), esa es la protección de los registros que se hacen de manera general basados en un controlador de dominio En el control de riesgos se validad los log y se pasan al dispositivo del backup que se realiza		60	Documentar los lineamientos a travpes de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.4.4.3	Responsable de SI	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se debe registrar, y los registros se deben proteger y revisar con regularidad.	A.12.4.3		PR.PT-1 RS.AN-1	Revisar los registros de las actividades del administrador y del operador del sistema, los registros se deben proteger y revisar con regularidad.	Los registros se valoran a través de ORFEO (Confidencialidad, integralidad, disponibilidad), tambien a través del control de las cuentas (perfiles de los usuarios), esa es la protección de los registros que se hacen de manera general basados en un controlador de dominio En el control de riesgos se validad los log y se pasan al dispositivo del backup que se realiza		60	Documentar los lineamientos a travpes de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.4.4.4	Responsable de SI	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	A.12.4.4		PR.PT-1	Revisar se deberían sincronizar con una única fuente de referencia de tiempo Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.	De acuerdo a lo expuesto por el proceso en la matriz de autodiagnostico: La entidad es conciente de la necesidad de implementar el servicio de ntp para su infraestructura.		40	Gestionar y documentar el cumplimiento del criterio
T.4.5	**Responsable de TICs**	**CONTROL DE SOFTWARE OPERACIONAL**	**Asegurar la integridad de los sistemas operacionales.**	**A.12.5**	Modelo de madurez definido					**60**	
T.4.5.1	Responsable de TICs	Instalación de software en sistemas operativos	Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.	A.12.5.1		PR.DS-6 PR.IP-1 PR.IP-3 DE.CM-5	Revisar las siguientes directrices para control de software operacional: a) actualizar el software operacional, aplicaciones y bibliotecas de programas solo la debe llevar a cabo administradores entrenados, con autorización apropiada de la dirección; b) definir que los sistemas operacionales sólo debe contener códigos ejecutables aprobados, no el código de desarrollo o compiladores; c) establecer que las aplicaciones y el software del sistema operativo solo se debe implementar después de pruebas extensas y exitosas; los ensayos deben abarcar la usabilidad, la seguridad, los efectos sobre otros sistemas y la facilidad de uso, y se debe llevar a cabo en sistemas separados; se debe asegurar que todas las bibliotecas de fuentes de programas correspondientes hayan sido actualizadas; d) usar un sistema de control de la configuración para mantener el control de todo el software implementado, al igual que la documentación del sistema; e) establecer una estrategia de retroceso (rollback) antes de implementar los cambios; f) mantener un log de auditoría de todas las actualizaciones de las bibliotecas de programas operacionales;	En gran medida se gestiona sobre los ambientes de prueba (ORFEO), antes de pasar a producción o capacitaciones de hace en ambientes de prueba. El único gran sistema propio de la entidad es ORFEO y sobre la cual se cumplen los criterios evaluados. Los ambientes de producción no se afectan cuando se estan haciendo pruebas o desarrollos. Sin embargo se gestiona con la experticia de los funcionarios vinculados al proceso pero no se encuentra documentado		60	Documentar los lineamientos a travpes de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.4.6	**Responsable de SI**	**GESTIÓN DE LA VULNERABILIDAD TÉCNICA**	**Prevenir el aprovechamiento de las vulnerabilidades técnicas.**	**A.12.6**	Modelo de madurez gestionado					**80**	
T.4.6.1	Responsable de SI	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades,	A.12.6.1		ID.RA-1 ID.RA-5 PR.IP-12 DE.CM-8 RS.MI-3	Revisar las siguientes directrices para vulnerabilidades técnicas: a) definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida; b) definir los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellos se debe identificar para el software y otra tecnología;	De manera general se evidencia a través de la Política de Seguridad de la Información, no obstante no se encuentran documentados todos los criterios evaluados en este item		60	Documentar los lineamientos a travpes de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.4.6.2	Responsable de TICs	Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	A.12.6.2		PR.IP-1 PR.IP-3	Revisar las restricciones y las reglas para la instalación de software por parte de los usuarios.	De acuerdo a lo observado en el seguimiento realizado al cumplimiento de Derechos de Autor se identificaron los siguientes documentos: • Guía Metodológica de gestión de activos de información (Código GT-GU-01 Versión 2). 8. POLÍTICAS PARA EL USO ACEPTABLE DE LOS ACTIVOS: Usos no autorizados: Está prohibido realizar cambios a los activos informáticos de la Fundación Gilberto Álzate, sin contar con la autorización formal del responsable de las áreas o del proceso en el que esté el activo informático", "No debe cambiar ni alterar de ninguna forma el hardware o el software de los sistemas de información de la Fundación Gilberto Álzate" y "Los funcionarios deben cumplir con los derechos de autor y los contratos de licencia" • Políticas de Seguridad de la Información (GTI-POL-01) Versión 1 del 13/02/2017. 8. MANEJO DE ACCESO A INTERNET – "Queda prohibida la descarga que no cumpla con la normatividad vigente de copyright y similar". Ver informe cumplimiento Derechos de Autor 2019		100	
T.4.7	**Responsable de TICs**	**CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN**	**Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.**	**A.12.7**	Modelo de madurez gestionado cuantitativamente					**n/a**	
T.4.7.1	Responsable de TICs	Controles sobre auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se debe planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	A.12.7.1			Revisar las siguientes directrices para las auditorias de sistemas de información: a) establecer los requisitos de auditoría para acceso a sistemas y a datos se debe acordar con la dirección apropiada; b) definir el alcance de las pruebas técnicas de auditoría se debe acordar y controlar; c) establecer las pruebas de auditoría se debe limitar a acceso a software y datos únicamente para lectura; d) definir el acceso diferente al de solo lectura solamente se debe prever para copias aisladas de los archivos del sistema, que se deben borrar una vez que la auditoría haya finalizado, o se debe proporcionar información apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría; e) definir los requisitos para procesos especiales y adicionales se debe identificar y acordar; f) establecer las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales; g) hacer seguimiento de todos los accesos y logged para producir un rastro de referencia.	No aplica		n/a	
SEGURIDAD DE LAS COMUNICACIONES											
T.5	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS COMUNICACIONES**		**A.13**						47	
T.5.1	**Responsable de TICs**	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**	**Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.**	**A.13.1**	Modelo de madurez definido					**53**	
T.5.1.1	Responsable de TICs	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1		PR.AC-3 PR.AC-5 PR.DS-2 PR.PT-4	Revisar las siguientes directrices para la gestión de seguridad de redes: a) establecer las responsabilidades y procedimientos para la gestión de equipos de redes; b) definir la responsabilidad operacional por las redes se debería separar de las operaciones informáticas, en donde sea apropiado; c) establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre redes inalámbricas, y para proteger los sistemas y aplicaciones conectados; d) De acuerdo a NIST, Gestionar el acceso remoto d) aplicar logging y seguimiento adecuados para posibilitar el registro y detección de acciones que pueden afectar, o son pertinentes a la seguridad de la información; e) definir las actividades de gestión a coordinar estrechamente tanto para optimizar el servicio de la organización, como para	Se evidencian los documentos: * Políticas de Seguridad de la Información * Políticas internas de Seguridad y tratamiento de datos. * Procedimiento Seguridad de Redes No se evidencia de manera clara como se da cumplimiento a los criterios aquí evaluados.		60	Documentar los lineamientos a travpes de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.5.1.2	Responsable de SI	Seguridad de los servicios de red	Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	A.13.1.2			Revisar las siguientes directrices para la seguridad de los servicios de red: a) establecer la tecnología aplicada a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red; b) definir los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red; c) establecer los procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.	Se evidencian los documentos: * Políticas de Seguridad de la Información * Políticas internas de Seguridad y tratamiento de datos. * Procedimiento Seguridad de Redes No se evidencia de manera clara como se da cumplimiento a los criterios aquí evaluados.		60	Documentar los lineamientos a travpes de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.5.1.3	Responsable de TICs	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	A.13.1.3		PR.AC-5 PR.DS-5	De acuerdo a NIST se debe proteger la integridad de las redes incorporando segregación donde se requiera.	La segmentación en la IPV4 pero hay ina directirz de migración a IPV6 por tanto se debe gestionar recursos para hacer la migración		40	Documentar los lineamientos a travpes de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.5.2	**Responsable de TICs**	**TRANSFERENCIA DE INFORMACIÓN**	**Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.**	**A.13.2**	Modelo de madurez definido					**40**	
T.5.2.1	Responsable de TICs	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	A.13.2.1		ID.AM-3 PR.AC-5 PR.AC-3 PR.DS-2 PR.DS-5 PR.PT-4	De acuerdo a la NIST: Se deben mapear los flujos de comunicaciones y datos para poder cumplir con este ítem. Revisar las siguientes directrices: a) definir los procedimientos diseñados para proteger la información transferida contra interceptación, copiado, modificación, enrutado y destrucción; b) definir los procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas;	Se identican controles documentados de criterios, de acuerdo a lo expuesto por el proceso en la matriz de autodiagnostico: La entidad conoce el riesgo y procedera a la implementación. Se realiza implementación servicio firewall.		40	Documentar los lineamientos a travpes de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.5.2.2	Responsable de TICs	Acuerdos sobre transferencia de información	Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	A.13.2.2			Revisar las siguientes directrices para transferencia segura de la información: a) establecer las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo; b) definir los procedimientos para asegurar trazabilidad y no repudio; c) definir los estándares técnicos mínimos para empaquetado y transmisión; d) tener certificados de depósito de títulos en garantía; e) establecer los estándares de identificación de mensajería; f) definir las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos; g) establecer el uso de un sistema de etiquetado acordado para información sensible o crítica, que asegure que el significado de la	El proceso indica en la matriz de autodiagnostico: La entidad conoce el riesgo y procedera a la implementación. NO se encuentran documentados de manera clara todos los criterios evaluados en este ítem		20	Documentar los lineamientos a travpes de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.5.2.3	Responsable de TICs	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	A.13.2.3		PR.DS-2 PR.DS-5	Revisar las siguientes directrices para mensajería electrónica: a) definir la protección de mensajes contra acceso no autorizado, modificación o denegación del servicio proporcionales al esquema de clasificación adoptado por la organización; b) asegurar el direccionamiento y transporte correctos del mensaje; c) establecer la confiabilidad y disponibilidad del servicio; d) definir las consideraciones legales, (los requisitos para firmas electrónicas; e) establecer la obtención de aprobación antes de usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información); f) definir niveles más fuertes de autenticación para control del acceso desde redes accesibles públicamente.	Se evidencia que se hace referencia a la mensajería electrónica en los documentos: Políticas de Seguridad de la Información - 6. SEGURIDAD DE LAS CUENTAS DE CORREO ELECTRÓNICO No obstante no se identifica de manera clara como se da cumplimiento a los requisitos b a e		40	Documentar los lineamientos a través de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.5.2.4	Responsable de SI	Acuerdos de confidencialidad o de no divulgación	Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	A.13.2.4		PR.DS-5	Revisar las siguientes directrices para acuerdos de confidencialidad: a) definir la información que se va a proteger (información confidencial); b) determinar la duración esperada de un acuerdo, incluidos los casos en los que podría ser necesario mantener la confidencialidad indefinidamente; c) establecer las acciones requeridas cuando termina el acuerdo; d) definir las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información; e) definir la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de información confidencial; f) definir el uso permitido de información confidencial y los derechos del firmante para usar la información; g) establecer el derecho a actividades de auditoría y de seguimiento que involucran información confidencial; h) definir el proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial; i) definir los plazos para que la información sea devuelta o destruida al cesar el acuerdo; j) establecer las acciones que se espera tomar en caso de violación del acuerdo.	Si hay acuerdos de confidencialidad a través de los clausulados de los contratos y Gestión de Talento Humano, no obstante la documentación de los criterios tal como se encuentran definidos en este ítem no se encuentran establecidos de manera clara ni articulados entre los procesos vinculados (OAJ, GTH y Seguridad de la Información)		60	Documentar los lineamientos a travpes de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS											
T.6	**Responsable de SI/Responsable de TICs**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		**A.14**						34	
T.6.1	**Responsable de SI**	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**	**Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.**	**A.14.1**	Modelo de madurez definido					**40**	
T.6.1.1	Responsable de SI	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se debe incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	A.14.1.1		PR.IP-2	Revisar las siguientes directrices para análisis y especificaciones de requisitos de seguridad de la información: a) establecer el nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario. b) definir los procesos de suministro de acceso y de autorización para usuarios del negocio, al igual que para usuarios privilegiados o técnicos; c) informar a los usuarios y operadores sobre sus deberes y responsabilidades; d) definir las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad, integridad;	De acuerdo a lo indicado por el proceso en la matriz de autodiganostico: La entidad es conciente de la necesidad de implementar el servicio de ntp para su infraestructura.		40	Documentar los lineamientos a través de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.6.1.2	Responsable de SI	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2		PR.DS-2 PR.DS-5 PR.DS-6	Revisar las siguientes directrices para la seguridad de servicios de las aplicaciones en redes públicas: a) definir el nivel de confianza que cada parte requiere con relación a la identidad declarada por la otra parte, (por medio de autenticación); b) establecer los procesos de autorización asociados con quien puede aprobar el contenido o expedir o firmar documentos transaccionales clave; c) asegurar que los socios de comunicación estén completamente informados de sus autorizaciones para suministro o uso del servicio;	Si bien de manera general se vinculan algunos de los criterios establecidos en los documentos SIG del proceso (politica, procedimientos, entre otros), los mismo no se encuentran documentados conforme lo establecido		40	Documentar los lineamientos a través de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.6.1.3	Responsable de SI	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	A.14.1.3		PR.DS-2 PR.DS-5 PR.DS-6	Revisar las siguientes directrices protección de transacciones de los servicios de las aplicaciones: a) definir el uso de firmas electrónicas por cada una de las partes involucradas en la transacción; b) establecer todos los aspectos de la transacción, es decir, asegurar que: 1) definir la información de autenticación secreta de usuario, de todas las partes, se valide y verifique; 2) definir a transacción permanezca confidencial; 3) mantener la privacidad asociada con todas las partes involucradas; c) definir la trayectoria de las comunicaciones entre todas las partes involucradas esté encriptada; d) definir los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados; e) asegurar que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente, (en	Si bien la entidad hace uso de firmas electrónicas con la vinculación a sistemas de información de la Contraloria de Bogota (Sivicof) y Bancos, las directrices de protección se definen directamente con los propietarios de estos sistema		80	Documentar los lineamientos a través de los cuales se lleva a cabo el cumplimiento del requisito del item d)
T.6.2	**Responsable de SI**	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE**		**A.14.2**	Modelo de madurez definido					**43**	
T.6.2.1	Responsable de SI	Política de desarrollo seguro	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	A.14.2.1		PR.IP-2	Revisar las siguientes directrices política de desarrollo seguro: a) definir la seguridad del ambiente de desarrollo; b) orientar la seguridad en el ciclo de vida de desarrollo del software: 1) definir la seguridad en la metodología de desarrollo de software; 2) establecer las directrices de codificación seguras para cada lenguaje de programación usado; c) definir los requisitos de seguridad en la fase diseño;	Hay listas de chequeo y se vinculan con el procedimiento Implementación de soluciones y servicios de Tecnología, no obstante no se documentan de manera clara los criterios evaluados en este ítem		40	Documentar los lineamientos a través de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.6.2.2	Responsable de TICs	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se debe controlar mediante el uso de procedimientos formales de control de cambios.	A.14.2.2		PR.IP-1 PR.IP-3	Revisar las siguientes directrices procedimientos control de cambio en sistemas: a) llevar un registro de los niveles de autorización acordados; b) asegurar que los cambios se presenten a los usuarios autorizados; c) revisar los controles y procedimientos de integridad para asegurar que no se vean comprometidos por los cambios; d) identificar todo el software, información, entidades de bases de datos y hardware que requieren corrección; e) identificar y verificar el código crítico de seguridad para minimizar la posibilidad de debilidades de seguridad conocidas; f) obtener aprobación formal para propuestas detalladas antes de que el trabajo comience;	Hay listas de chequeo y se vinculan con el procedimiento Implementación de soluciones y servicios de Tecnología, no obstante no se documentan de manera clara los criterios evaluados en este ítem		40	Documentar los lineamientos a través de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.6.2.3	Responsable de TICs	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	A.14.2.3		PR.IP-1	Revisar las siguientes directrices revisión técnica de las aplicaciones después de cambios en la plataforma de operación: a) revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones; b) asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación; c) asegurar que se hacen cambios apropiados en los planes de continuidad del negocio.	El cumplimiento de estos criterios de vinculan con el desarrollo del item anterior		n/a	
T.6.2.4	Responsable de TICs	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	A.14.2.4		PR.IP-1	Revisar las siguientes directrices restricciones en los cambios a los paquetes de software: a) definir el riesgo de que los procesos de integridad y los controles incluidos se vean comprometidos; b) obtener el consentimiento del vendedor; c) obtener del vendedor los cambios requeridos, a medida que se actualiza el programa estándar; d) evaluar el impacto, si la organización llega a ser responsable del mantenimiento futuro del software como resultado de los cambios; e) definir la compatibilidad con otro software en uso.	Se vincula contractualmente, indicando en el clausulado de manera general el cumplimiento de estos criterios (Contratos de firewall, antivirus y el creativecloud) NO obstante no se evidencia documentación que haga referencia a los criterios tal como se establecen en el ítem		40	Documentar los lineamientos a través de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.

T.6.2.5	Responsable de TICs	Principios de construcción de sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	A.14.2.5		PR.IP-2	Revisar la documentación y los principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	Se vincula contractualmente, indicando en el clausulado de manera general el cumplimiento de estos criterios (Contratos de firewall, antivirus y el creativecloud) NO obstante no se evidencia documentación que haga referencia a los criterios tal como se establecen en el ítem		40	Documentar los lineamientos a través de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.6.2.6	Responsable de TICs	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	A.14.2.6			Revisar las siguientes directrices para ambiente de desarrollo seguro: a) carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir; b) definir los requisitos externos e internos aplicables, (reglamentaciones o políticas); c) definir los controles de seguridad ya implementados por la organización, que brindan soportar al desarrollo del sistema; d) establecer la confiabilidad del personal que trabaja en el ambiente; e) definir el grado de contratación externa asociado con el desarrollo del sistema; f) definir la necesidad de separación entre diferentes ambientes de desarrollo; g) definir el control de acceso al ambiente de desarrollo; h) establecer el seguimiento de los cambios en el ambiente y en los códigos almacenados ahí; i) definir las copias de respaldo se almacenan en lugares seguros fuera del sitio; j) definir el control sobre el movimiento de datos desde y hacia el ambiente.	Se vincula contractualmente, indicando en el clausulado de manera general el cumplimiento de estos criterios (Contratos de firewall, antivirus y el creativecloud) NO obstante no se evidencia documentación que haga referencia a los criterios tal como se establecen en el ítem		40	Documentar los lineamientos a través de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.6.2.7	Responsable de TICs	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	A.14.2.7		DE.CM-6	Revisar las siguientes directrices desarrollo contratado externamente: a) definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente; b) establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas; c) definir el suministro del modelo de amenaza aprobado, al desarrollador externo; d) realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables; e) definir la evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad; f) definir la evidencia de que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega.	La entidad no compra software a la medida propiamente por costos, lo que se hace es adaptar lo que esta en la red al funcionamiento de la entidad (ORFEO - Software libre). Los criterios se establecen en los clausulados de los contratos, de acuerdo a las necesidades de las áreas funcionales que requieren los sistemas.		60	Evaluar la pertinencia de la aplicabilidad de los criterios establecidos de conformidad con la realidad institucional y documentar
T.6.2.8	Responsable de SI	Pruebas de seguridad de sistemas	Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.	A.14.2.8	Modelo de madurez gestionado cuantitativamente	DE.DP-3	Verifique en una muestra que para pasar a producción los desarrollos se realizan pruebas de seguridad. También verifique que los procesos de detección de incidentes son probados periódicamente.	Esta en proceso la gestión de desarrollo en ORFEO		n/a	
T.6.2.9	Responsable de TICs	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados.	A.14.2.9			Revisar las pruebas de aceptación de sistemas, para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Esta en proceso la gestión de desarrollo en ORFEO		n/a	
T.6.3	Responsable de SI	**DATOS DE PRUEBA**	**Asegurar la protección de los datos usados para pruebas.**	**A.14.3**	Modelo de madurez definido					**20**	
T.6.3.1	Responsable de SI	Protección de datos de prueba	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	A.14.3.1			Revisar las siguientes directrices para protección de datos de prueba: a) establecer los procedimientos de control de acceso, que se aplican a los sistemas de aplicación operacionales, se debe aplicar también a los sistemas de aplicación de pruebas; b) tener una autorización separada cada vez que se copia información operacional a un ambiente de pruebas; c) definir que la información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas; d) establecer que el copiado y uso de la información operacional se debe logged para suministrar un rastro de auditoría.	De acuerdo a lo indicado en la aplicación de la lista de verifiación se conoce la necesidad y esta en proceso de documentación		20	Documentar los lineamientos a través de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN											
T.7.	**Responsable de SI/Responsable de TICs**	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		**A.16**						56	
T.7.1	**Responsable de SI**	**GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**	**Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.**	**A.16.1**						**56**	
T.7.1.1	Responsable de SI	Responsabilidades y procedimientos	Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	A.16.1.1		PR.IP-9 DE.AE-2 RS.CO-1	Revisar las siguientes directrices responsabilidades y procedimientos: a) establecer las responsabilidades de gestión, para asegurar que los siguientes procedimientos se desarrollan y comunican adecuadamente dentro de la organización: 1) los procedimientos para la planificación y preparación de respuesta a incidentes; 2) los procedimientos para seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información; 3) los procedimientos para logging las actividades de gestión de incidentes; 4) los procedimientos para el manejo de evidencia forense; 5) los procedimientos para la valoración y toma de decisiones sobre eventos de seguridad de la información y la valoración de debilidades de seguridad de la información; 6) los procedimientos para respuesta, incluyendo aquellos para llevar el asunto a una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas;	Se evidencia a través del procedimiento Gestión de Incidentes, Amenazas y Debilidades de Seguridad, sin embargo en el mismo no se define de manera clara como se cumplen los criterios evaluados		60	Evaluar la pertinencia de la aplicabilidad de los criterios establecidos de conformidad con la realidad institucional y documentar De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en la ***Guia No 21 Para la Gestión y Clasificación de Incidentes de Seguridad de la Información***
T.7.1.2	Responsable de SI	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se debe informar a través de los canales de gestión apropiados, tan pronto como sea posible.	A.16.1.2	Modelo de madurez definido	DE.DP-4	Revisar las siguientes directrices reporte de eventos de seguridad de la información: a) establecer un control de seguridad ineficaz; b) definir la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información; c) definir los errores humanos; d) definir las no conformidades con políticas o directrices; e) definir las violaciones de acuerdos de seguridad física; f) establecer los cambios no controlados en el sistema; g) definir mal funcionamiento en el software o hardware; h) definir violaciones de acceso. **Tenga en cuenta para la calificación:** 1) Si se elaboran informes de TODOS los incidentes de seguridad y privacidad de la información, TODOS están documentados e incluidos en el plan de mejoramiento continuo. Se definen los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro, están en 40. 2) Si los controles y medidas identificados para disminuir los incidentes fueron implementados, están en 60.	Se evidencia a través del procedimiento Gestión de Incidentes, Amenazas y Debilidades de Seguridad, sin embargo en el mismo no se define de manera clara como se cumplen los criterios evaluados De acuerdo a lo indicado en la aplicación de la lista de verificación se elaboran los informes y se documenta y presentan en el Comite de Desempeño.		40	Evaluar la pertinencia de la aplicabilidad de los criterios establecidos de conformidad con la realidad institucional y documentar De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en la ***Guia No 21 Para la Gestión y Clasificación de Incidentes de Seguridad de la Información***
T.7.1.3	Responsable de SI	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de	A.16.1.3	Modelo de madurez definido	RS.CO-2	Observe si los eventos son reportados de forma consistente en toda la entidad de acuerdo a los criterios establecidos.	Se hace a través de la mesa de ayuda. El reporte no presenta incidentes de seguridad		100	
T.7.1.4	Responsable de SI	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se debe evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	A.16.1.4	Madurez Inicial	DE.AE-2 RS.AN-4	Revise si los eventos de SI detectados son analizados para determinar si constituyen un incidentes de seguridad de la información y entender los objetivos del ataque y sus métodos. Evidencia si los incidentes son categorizados y se cuenta con planes de respuesta para cada categoría.	NO se presentaron incidentes de seguridad en el periodo auditado.		n/a	
T.7.1.5	Responsable de SI	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	A.16.1.5	Modelo de madurez gestionado cuantitativamente	RS.RP-1 RS.AN-1 RS.MI-2 RC.RP-1 RC.RP-1	Revisar las siguientes directrices para respuesta a incidentes de seguridad de la información: a) Los incidentes son contenidos y la probabilidad de que vuelvan a ocurrir mitigada. b) Se debe contar con un plan de recuperación de incidentes durante o después del mismo. b) recolectar evidencia lo más pronto posible después de que ocurra el incidente; c) llevar a cabo análisis forense de seguridad de la información, según se requiera d) llevar el asunto a una instancia superior, según se requiera;	Se evidencia a través del procedimiento Gestión de Incidentes, Amenazas y Debilidades de Seguridad, sin embargo en el mismo no se define de manera clara como se cumplen los criterios evaluados		40	Documentar los lineamientos a través de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.7.1.6	Responsable de TICs	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	A.16.1.6	Modelo de madurez gestionado cuantitativamente	DE.DP-5 RS.AN-2 RS.IM-1	De acuerdo a la NIST se debe entender cual fue el impacto del incidente. Las lecciones aprendidas deben ser usadas para actualizar los planes de respuesta a los incidentes de SI. **Tenga en cuenta para la calificación:** La Entidad aprende continuamente sobre los incidentes de seguridad presentados.	Se evidencia a través del procedimiento Gestión de Incidentes, Amenazas y Debilidades de Seguridad, sin embargo en el mismo no se define de manera clara como se cumplen los criterios evaluados		40	Documentar los lineamientos a través de los cuales se lleva a cabo el cumplimiento de lso requisitos definidos.
T.7.1.7	Responsable de TICs	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	A.16.1.7	Modelo de madurez gestionado Modelo de madurez definido	RS.AN-3	Revisar las siguientes directrices para recolección de evidencia: a) definir la cadena de custodia; b) establecer la seguridad de la evidencia; c) definir la seguridad del personal; d) definir los roles y responsabilidades del personal involucrado; e) establecer la competencia del personal; f) realizar la documentación; g) definir las sesiones informativas.	NO aplica para la entidad por cuanto la gestión del levantamiento de información en un evento critico se desarrolla a través del Colcert (Organismo encargado de los temas de seguridad a nivel de Colombia)		n/a	

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

FUNDACIÓN GILBERTO ALZATE AVENDAÑO

COMPONENTE	ID	CARGO	ITEM	DESCRIPCIÓN	PRUEBA	CIBERSEGURIDAD	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO PHVA	RECOMENDACIÓN
	P.1	Responsable SI	Alcande MSPI (Modelo de Seguridad y Privacidad de la Información)	Se debe determinar los límites y la aplicabilidad del SGSI para establecer su alcance.	Solicite el documento del alcance que debe estar apobado, socializado al interior de la Entidad, por la alta dirección. Determine si en la definición del alcance se considerará: 1) Aspectos internos y externos referidos en el 4.1.: La Entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el SGSI. Nota. La terminación de estos aspectos hace referencia a establecer el contexto interno y externo de la empresa, referencia a la norma ISO 31000:2009 en el apartado 5.3. 2) Los requisitos referidos en 4.2.: a. Se debe determinar las partes interesadas que son pertinentes al SGSI. b. Se debe determinar los requisitos de las partes interesadas. Nota. Los requisitos pueden incluir los requisitos legales y de reglamentación y las obligaciones contractuales. 3) Las interfaces y dependencias entre las actividades realizadas y las que realizan otras entidades del gobierno nacional o entidades exteriores		componente planificación	En el documento Políticas de Seguridad de la Información no se identifican los criterios aquí establecidos. No se evidencia que se identifica de manera clara el alcance del SGSI conforme lo establece la norma tcnica 27001 numeral 4,1		60	Documentar como se da cumplimiento a los requisitos establecidos para este criterio e identificarlos dentro de la politica establecida.
	P.2		Políticas de seguridad y privacidad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a la partes externas pertinentes	Solicite la política de seguridad de la información de la entidad y evalúe: a) Si se definen los objetivos, alcance de la política b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección Revise si la política: a)Define que es seguridad de la información b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos; c) Los procesos para manejar las desviaciones y las excepciones. Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas. Verifique cada cuanto o bajo que circunstancias se revisan y actualizan, verifique la ultima fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual. Para la calificación tenga en cuenta que: 1) Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, están en 20. 2) Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, , están en 40. 3) Si se divulgan las políticas de seguridad y privacidad de la información, están en 60.		componente planificación			60 40	Conforme lo observado se recomienda revisar y de considerarse pertinente ajustar el documento teniendo en cuenta las bases indicadas por MINTIC en la Guia No.2. Elaboración de la política general de seguridad y privacidad de la información, asegurando la incorporación de los requisitos señalados en el campo EVIDENCIA 0
	P.3	Calidad	Procedimientos de control documental del MSPI	La información documentada se debe controlar para asegurar que: a. Esté disponible y adecuado para su uso, cuando y donde se requiere b. Esté protegida adecuadamente.	Solicite Formatos de procesos y procedimienos debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de gestión institucional, por ejemplo el sistema de calidad SGC. Verifique: 1) Cómo se controla su distribución, acceso, recuperación y uso 2) Cómo se almacena y se asegura su preservación 3) Cómo se controlan los cambios		componente planificación	Se evidencia a través de los documentos SIG vinculados al proceso los cuales se encuentran en la intranet de la entidad en la siguiente ruta. http://intranet.fuga.gov.co/proceso-gestion-de-tecnologia.		100	
	P.4	Responsable SI	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (ó e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección. Revise la estructura del SGSI: 1) Tiene el SGSI suficiente apoyo de la alta dirección?, esto se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes. 2) Están claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas?, 3) Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección) 4)Estan definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales? 5) Estan definidos y documentados los niveles de autorización? 6) Se cuenta con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo campañas de sensibilización en seguridad de la información)		componente planificación			20	De acuerdo a lo observado en el campo EVIDENCIAS y teniendo en cuenta que la implementación del Modelo corresponde a una gestión institucional que involucra de manera transversal a varios procesos de la entidad; se recomienda desde la Alta Dirección definir los roles y responsabilidades conforme los temas que deben considerarse en el MSPI (Referencia Hoja Areas Involucradas del presente instrumento) De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en la Guia No.4. Roles y Responsablidades

PLANIFICACIÓN	P.5	Responsable SI	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Solicite el inventario de activos de información, revisado y aprobado por la alta Dirección y revise: 1) Ultima vez que se actualizó 2) Que señale bajo algún criterio la importancia del activo 3) Que señale el propietario del activo Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión. De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos. Tenga en cuenta para la calificación: 1) Si Se identifican en forma general los activos de información de la Entidad, están en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, están en 60. 3) Si se revisa y monitorean periódicamente los activos de información de la entidad, están en 80.		componente planificación			60	Fortalecer los controles de tal manera que la información relacionada con el inventario de activos Software, hardware y servicios de encuentre actualizada. De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC: Guia No.2. Elaboración de la política general de seguridad y privacidad de la información Guia No 5 Gestión Clasificación de Activos
	P.6	Responsable SI	Identificación y valoración de riesgos	Metodología de análisis y valoración de riesgos e informe de análisis de riesgos	1) Solicite a la entidad la metodología y criterios de riesgo de seguridad, aprobado por la alta Dirección que incluya: 1. Criterios de Aceptación de Riesgos o tolerancia al riesgo que han sido informados por la alta Dirección. 2. Criterios para realizar evaluaciones de riesgos. 2) Solicite los resultados de las evaluaciones de riesgos y establezca: a. Cuantas evaluaciones repetidas de riesgos se han realizado y que sus resultados consistentes, válidos y comparables. b. Que se hayan identificado los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad de la información dentro del alcance. c. Que se hayan identificado los dueños de los riesgos. d. Que se hayan analizado los riesgos es decir: - Evaluado las consecuencias (impacto) potenciales si se materializan los riesgos identificados - Evaluado la probabilidad realista de que ocurran los riesgos identificados - Determinado los niveles de riesgo. e. Que se hayan evaluado los riesgos es decir: - Comparado los resultados del análisis de riesgos con los criterios definidos - Priorizado los riesgos analizados para el tratamiento de riesgos.	ID.RA-5 ID.RM-1 ID.RM-2 ID.RM-3	componente planificación	La Metodología de análisis y valoración de riesgos e informe de análisis de riesgos definida en la entidad se evidencia a través del documento Política de administración del riesgo (CEM-PO-01) Versión 2, documento que hace refernicia a los riesgos de seguridad digital, no obstante no se evidencia en el documento que se identique de manera especifica los criterios que aplican de manera particular a los riegos de seguridad digital (amenazas, vulnerabilidades, activos de información vinculados, criterios de impacto)		60	A través de la Oficina Asesora de Planeación revisar, ajustar e implementar las particulares a los riesgos de seguridad digital en la política de administración de riesgo y la metodologia de tal forma que se atienda lo dispuesto tanto por el Departamento de la Función Publica como por MINTIC en relación con este tema
	P.8	Responsable SI	Tratamiento de riesgos de seguridad de la información	Los riesgos deben ser tratados para mitigarlos y llevarlos a niveles tolerables por la Entidad	1) Solicite el plan de tratamiento de riesgos y la declaración de aplicabilidad verifique que: a. Se seleccionaron opciones apropiadas para tratar los riesgos, teniendo en cuenta los resultados de la evaluación de riesgos. b. Se determinaron todos los controles necesarios para implementar las opciones escogidas para el tratamiento de riesgos. c. Compare los controles determinados en el plan de tratamiento con los del Anexo A y verifique que no se han omitidos controles, si estos han sido omitidos se debe reflejar en la declaración de aplicabilidad. d. Revise la Declaración de Aplicabilidad que tenga los controles necesarios y la justificación de las exclusiones, ya sea que se implementen o no y la justificación para las exclusiones de los controles del Anexo A, y que haya sido revisado y aprobado por la alta Dirección. e. Revise que el plan de tratamiento de riesgos haya sido revisado y aprobado por la alta Dirección. f. Revise que exista una aceptación de los riesgos residuales por parte de los dueños de los riesgos.	ID.RA-6 ID.RM-1 ID.RM-2 ID.RM-3	Modelo de Seguridad y Privacidad de la Información, componente planificación	La Metodología de análisis y valoración de riesgos e informe de análisis de riesgos definida en la entidad se evidencia a través del documento Política de administración del riesgo (CEM-PO-01) Versión 2, documento que hace refernicia a los riesgos de seguridad digital, no obstante no se evidencia la Declaración de Aplicabilidad ni los criterios resaltados		60	Implementar y documentar la Declaración de Aplicabilidad De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en la ***Guia No. 8 Controles de seguridad y Privacidad de la Información***
	P.9	Responsable SI	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	Entreviste a los líderes de los procesos y pregunteles que saben sobre la seguridad de la información, cuales son sus responsabilidades y como aplican la seguridad de la información en su diario trabajo. Pregunte como se asegura que los funcionarios, Directores, Gerentes y contratistas tomen conciencia en seguridad de la información, alineado con las responsabilidades, políticas y procedimientos existentes en la Entidad. Solicite el documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección. Verifique que se han tenido en cuenta buenas prácticas como: a) Desarrollar campañas, elaborar folletos y boletines. b) Los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección c) Verifique que nuevos empleados y contratistas son objeto de sensibilización en SI. d) Indague cada cuanto o con que criterios se actualizan los programas de toma de conciencia. e) Verifique que en las evidencias se puede establecer los asistentes al programa y el tema impartido. f) Incluir en los temas de toma de conciencia los procedimientos básicos de seguridad de la información (tales como el reporte de incidentes de seguridad de la información) y los controles de línea base (tales como la seguridad de las contraseñas, los controles del software malicioso, y los escritorios limpios). g) De acuerdo a NIST verifique que los funcionarios con roles privilegiados entienden sus responsabilidades y roles. Para la calificación tenga en cuenta que: Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información. Diseñar programas para los conciencia y comunicación, de las políticas de seguridad y		componente planificación	Se identifica la debilidad y se proyecta la elaboración de un plan de comunicaciones que abarque estos criterios		20	Identificar de manera ingetral los requisitos que hacen parte de este criterio y documentarlos De considerarse pertinente se recomienda tener en cuenta las bases indicadas por MINTIC en la ***Guia No 14 Plan de Capacitación, sensibilización y comunicación de Seguridad de la Información***
PROMEDIO										**53**	**21,33333333**

IMPLEMENTACIÓN	I.1	Responsable SI	Planificación y control operacional	Estrategia que se debe ejecutar con las actividades para lograr la implementación y puesta en marcha del MSPI de la entidad.	Solicite y evalue el documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.		componente implementación	Se evidencia a través de la evaluación en el autodiagnostico del instrumento MSPI realizado por el proceso, no obstante en el ejercicio no se evidencias las estrategias adoptadas para implementar de manera integral el modelo en la entidad		40	Documentar las estrategias adoptadas y que estas cumplan con los requisitos establecidos en este criterio
	I.2	n/a	Implementación de controles	Grado de implementación de controles del Anexo A de la ISO 27001	N/A		componente implementación		N/A	58	N/A
	I.3	Responsable SI	Implementación del plan de tratamiento de riesgos	Porcentaje de avance en la ejecución de los planes de tratamiento	Verifique los compromisos de avance en el plan de tratamiento de riesgos y el grado de cumplimiento de los mismos y genere un dato con el porcentaje de avance.		componente implementación	Se evidencia plan de tratamiento para la vigencia 2019, no obstante esta en proceso de ajuste conforme lo normado		20	Documentar y gestionar
	I.4	Responsable SI	Indicadores de gestión del MSPI	Indicadores de gestión del MSPI definidos	Solicite los Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.		componente implementación	Si bien se evidencia los indicadores para la vigencia 2019, no se evidencia la aprobación de los mismos por parte de la alta dirección. Los indicadores de la vigencia 2020 se encuentran en proceso de		20	Documentar y gestionar
PROMEDIO										34,41071429	6,882142857
EVALUACIÓN DE DESEMPEÑO	E.1	Responsable SI	Plan de seguimiento, evaluación y análisis del MSPI	Plan para evaluar el desempeño y eficacia del MSPI a través de instrumentos que permita determinar la efectividad de la implantación del MSPI.	Solicite y evalue el documento con el plan de seguimiento, evaluación, análisis y resultadosdel MSPI, revisado y aprobado por la alta Dirección.		componente evaluación del desempeño	El seguimiento se realizo a través del autodiganostico presentado por el proceso en el comité Directivo en su sesión del mes de Diciembre de 2019		80	Incorporar el resultado del ejercicio realizado por la OCI e implementar plan de mejoramiento
	E.2	Control Interno	Auditoría Interna	Plan de auditoría interna	Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.		componente evaluación del desempeño	No se incluyo para la vigencia 2019 pero de acuerdo a la necesidad se incorporo en las actividades del PAAI de la vigencia 2020. La auditoria esta en ejecución		20	Documentar y gestionar
	E.3	Responsable SI	Evaluación del plan de tratamiento de riesgos	Evaluación y seguimiento a los compromisos establecidos para ejecutar el plan de tratamiento de riesgos.	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.		componente evaluación del desempeño	No se incluyo para la vigencia 2019 pero de acuerdo a la necesidad se incorporo en las actividades del PAAI de la vigencia 2020. La auditoria esta en ejecución		20	Documentar y gestionar
PROMEDIO										40	8
MEJORA CONTINUA	M.1	Responsable SI	Plan de seguimiento, evaluación y análisis del MSPI	Resultados consolidados del componente evaluación de desempeño	Solicite y evalue el documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.		componente mejora continua	Esta en ejecución		20	
	M.2	Control Interno	Auditoría Interna	Comunicación delos resultados y plan para subsanar los hallazgos y oportunidades de mejora.	Solicite el documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidaes de mejora se subsanen, para asegurar la mejora continua. **Tenga en cuenta para la calificación que:** 1) Elaboración de planes de mejora es 60 2) Se implementan las acciones correctivas y planes de mejora es 80		componente mejora continua	Esta en ejecución		20	
PROMEDIO										20	4

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

FUNDACIÓN GILBERTO ALZATE AVENDAÑO

ID REQUISITO	CARGO	REQUISITO	HOJA	ELEMENTO	CALIFICACIÓN OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	NIVEL 3 DEFINIDO	CUMPLIMIENTO NIVEL DEFINIDO	NIVEL 4 GESTIONADO CUANTITATIVAMENTE	CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE	NIVEL 5 OPTIMIZADO	CUMPLIMIENTO NIVEL 5 OPTIMIZADO
R1	n/a	1) Si Se identifican en forma general los activos de información de la Entidad, estan en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, estan en 60. 3) Si se revisa y monitorean periódicamente los activos de información de la entidad, estan en 80.	Administrativas	AD.4.1.1	60	40	MAYOR	60	CUMPLE	60	CUMPLE	80	MENOR	100	MENOR
R2	n/a	Se clasifican los activos de información lógicos y físicos de la Entidad.	Administrativas	AD.4.2.1	60	20	MAYOR	40	MAYOR	60	CUMPLE	80	MENOR	100	MENOR
R3	n/a	1. Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información y se han diseñado programas para los funcionarios de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, estan en 20. 2. Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, estan aprobados y documentados, por la alta Dirección, estan en 40. 3. Si se han ejecutado los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Dirección, , estan en 60.	Administrativas	AD.3.2.2	60	20	MAYOR	40	MAYOR	60	CUMPLE	80	MENOR	100	MENOR
R4	n/a	Existe la necesidad de implementar el Modelo de Seguridad y Privacidad de la Información, para definir políticas, procesos y procedimientos claros para dar una respuesta proactiva a las amenazas que se presenten en la Entidad.	PHVA	P.1	60	20	MAYOR	40	MAYOR	60	CUMPLE	80	MENOR	100	MENOR
			Administrativas	AD.1.1	60	20	MAYOR	40	MAYOR	60	CUMPLE	80	MENOR	100	MENOR
			PHVA	P.4	20	20	CUMPLE	40	MENOR	60	MENOR	80	MENOR	100	MENOR
R5	Responsable de SI	1. Si se tratan temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, coloque 20 2.Los temas de seguridad de la información se tratan en los comités directivos interdisciplinarios de la Entidad, con regularidad, coloque 40	Madurez	R5	60	20	MAYOR	40	MAYOR	60	CUMPLE	80	MENOR	100	MENOR
R6	n/a	1. Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, estan en 20. 2. Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, , estan en 40. 3. Si se divulgan las políticas de seguridad y privacidad de la información, estan en 60.	Administrativas	AD.1.1	60	20	MAYOR	40	MAYOR	60	CUMPLE	80	MENOR	100	MENOR

R7	n/a	Establecer y documentar el alcance, limites, política, procedimientos, roles y responsabilidades y del Modelo de Seguridad y Privacidad de la Información.	PHVA	P.1	60	60	CUMPLE	60	CUMPLE	60	CUMPLE	80	MENOR	100	MENOR
R8	n/a	Determinar el impacto que generan los eventos que atenten contra la integridad, disponibilidad y confidencialidad de la información de la Entidad.	Tecnicas	T.7.1.4	n/a	20	MAYOR	40	MAYOR	60	MAYOR	60	MAYOR	80	MAYOR
ITE DE MADUREZ INICIAL					500	260	CUMPLE	440	MENOR	600	MENOR	780	MENOR	980	MENOR
R9	Responsable de SI	Con base en el inventario de activos de información clasificado, se establece la caracterización de cada uno de los sistemas de información.	Madurez	R9	80	N/A	N/A	40	MAYOR	60	MAYOR	80	CUMPLE	100	MENOR
R10	n/a	Aprobación de la alta dirección, documentada y firmada, para la Implementación del Modelo de Seguridad y Privacidad de la Información.	Madurez	R9	80	N/A	N/A	60	MAYOR	60	MAYOR	80	CUMPLE	100	MENOR
R11	n/a	Identificar los riesgos asociados con la información, físicos, lógicos, identificando sus vulnerabilidades y amenazas.	PHVA	P.6	60	N/A	N/A	40	MAYOR	60	CUMPLE	80	MENOR	100	MENOR

R12	n/a	1) Si se elaboran informes de TODOS los incidentes de seguridad y privacidad de la información, TODOS estan documentados e incluidos en el plan de mejoramiento continuo.Se definen los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro, estan en 40. 2) Si los controles y medidas identificados para disminuir los incidentes fueron implementados, estan en 60.	Tecnicas	T.7.1.2	40	N/A	N/A	40	CUMPLE	60	MENOR	80	MENOR	100	MENOR
R13	n/a	1. Si se cuentan con procedimientos que indican a los funcionarios como manejar la información y los activos de información en forma segura. Se tienen documentados los controles físicos y lógicos que se han definido en la Entidad, con los cuales se busca preservar la seguridad y privacidad de la información, aprobado por la alta Dirección, estan en 40. 2. Si se han divulgado e implementado los controles físicos y lógicos que wse han definido en la entidad, con los cuales se busca preservar la seguridad y privacidad de la información, estan en 60.	Administrativas	AD.4.1	90	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	MENOR
R14	n/a	Si existen planes de continuidad del negocio que contemplen los procesos críticos de la Entidad que garanticen la continuidad de los mismos. Se documentantan y protegen adecuadamente los planes de continuidad del negocio de la Entidad, este de estar documentado y firmado, por la alta Dirección, estan en 40. Si se reconoce la importancia de ampliar los planes de continuidade del negocio a otros procesos, pero aun no se pueden incluir ni trabajar con ellos, estan en 60.	Administrativas	AD.5.1.1	20	N/A	N/A	40	MENOR	60	MENOR	80	MENOR	100	MENOR
R15	n/a	Los roles de seguridad y privacidad de la información están bien definidos y se lleva un registro de las actividades de cada uno.	Administrativas	AD.2.1	84	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	MENOR
R16	n/a	Dispositivos para movilidad y teletrabajo	Administrativas	AD.2.2	70	N/A	N/A	40	MAYOR	60	MAYOR	80	MENOR	100	MENOR
R17	n/a	Protección contra código malicioso	Tecnicas	T.4.2	60	N/A	N/A	40	MAYOR	60	CUMPLE	80	MENOR	100	MENOR
R18	n/a	Copias de seguridad	Tecnicas	T.4.3	60	N/A	N/A	40	MAYOR	60	CUMPLE	80	MENOR	100	MENOR
R19	n/a	Gestión de la vulnerabilidad técnica	Tecnicas	T.4.6	80	N/A	N/A	40	MAYOR	60	MAYOR	80	CUMPLE	100	MENOR
DE MADUREZ GESTIONADO					724	0		460	MENOR	660	MENOR	880	MENOR	1100	MENOR
R20	n/a	Seguridad ligada a los recursos humanos, antes de la contratación	Administrativas	AD.3.1	80	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE	100	MENOR
R21	n/a	Seguridad ligada a los recursos humanos, durante la contratación	Administrativas	AD.3.2	33	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R22	n/a	Seguridad ligada a los recursos humanos, al cese o cambio de puesto de trabajo	Administrativas	AD.3.3	40	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R23	n/a	Requisitos de negocio para el control de accesos.	Tecnicas	T.1.1	50	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR

R24	n/a	Responsabilidades del usuario frente al control de accesos	Tecnicas	T.1.2.6	80	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE	100	MENOR
R25	n/a	Seguridad física y ambiental en áreas seguras	Tecnicas	T.1.3.1	80	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE	100	MENOR
R26	n/a	Seguridad física y ambiental de los equipos	Tecnicas	T.3.2	69	N/A	N/A	N/A	N/A	60	MAYOR	80	MENOR	100	MENOR
R27	n/a	Responsabilidades y procedimientos de operación	Tecnicas	T.4.1	30	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R28	n/a	Seguridad en la operativa, control del software en explotación	Tecnicas	T.4.5	60	N/A	N/A	N/A	N/A	60	CUMPLE	80	MENOR	100	MENOR
R29	n/a	Gestión de la seguridad en las redes.	Tecnicas	T.5.1	53	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R30	n/a	Intercambio de información con partes externas	Tecnicas	T.5.2	40	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R31	n/a	Adquisición, desarrollo y mantenimiento de los sistemas de información, requisitos de seguridad de los sistemas de información.	Tecnicas	T.6.1	40	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R32	n/a	Adquisición, desarrollo y mantenimiento de los sistemas de información, seguridad en los procesos de desarrollo y soporte.	Tecnicas	T.6.2	43	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R33	n/a	Adquisición, desarrollo y mantenimiento de los sistemas de información, datos de prueba.	Tecnicas	T.6.3	20	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR

R34	n/a	Gestión de incidentes en la seguridad de la información, notificación de los eventos de seguridad de la información.	Tecnicas	T.7.1.2	40	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R35	n/a	Gestión de incidentes en la seguridad de la información, notificación de puntos débiles de la seguridad.	Tecnicas	T.7.1.3	100	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	CUMPLE
R36	n/a	Gestión de incidentes en la seguridad de la información, recopilación de evidencias.	Tecnicas	T.7.1.7	n/a	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	MAYOR
R37	n/a	Implantación de la continuidad de la seguridad de la información.	Administrativas	AD.5.1.2	20	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R38	Responsable de compras y adquisiciones	Seguridad de la información en las relaciones con suministradores.	Administrativas	AD.7.1	80	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE	100	MENOR
R39	Responsable de compras y adquisiciones	Gestión de la prestación del servicio por suministradores.	Administrativas	AD.7.2	100	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	CUMPLE
R40	n/a	Se implementa el plan de tratamiento de riesgos y las medidas necesarias para mitigar la materialización de las amenazas.	PHVA	P.8	60	N/A	N/A	N/A	N/A	60	CUMPLE	80	MENOR	100	MENOR
TE DE MADUREZ DEFINIDO					543	0		0		660	MENOR	880	MENOR	1100	MENOR
R41	n/a	Se utilizan indicadores de cumplimiento para establecer si las políticas de seguridad y privacidad de la información y las clausulas establecidas por la organización en los contratos de trabajo, son acatadas correctamente. Se deben generar informes del desempeño de la operación del MSPI, con la medición de los indicadores de gestión definidos.	PHVA	I.5	#N/A	N/A	N/A	N/A	N/A	N/A	N/A	60	#N/A	80	#N/A
			PHVA	E.1	80	N/A	N/A	N/A	N/A	N/A	N/A	40	MAYOR	60	MAYOR
			PHVA	E.2	20	N/A	N/A	N/A	N/A	N/A	N/A	40	MENOR	60	MENOR
			PHVA	E.3	20	N/A	N/A	N/A	N/A	N/A	N/A	40	MENOR	60	MENOR
			PHVA	M.1	20	N/A	N/A	N/A	N/A	N/A	N/A	40	MENOR	60	MENOR

R42	n/a	Se realizan pruebas de manera sistemática a los controles, para determinar si están funcionando de manera adecuada. Se deben generar informes del desempeño de la operación del MSPI, con la revisión y verificación continua de los controles implementados. Tambien se generan informes de auditorías de acuerdo a lo establecido en el plan de auditorías de la entidad. Se realizan pruebas de efectividad en la Entidad, para detectar vulnerabilidades (físicas, lógicas y humanas) y accesos no autorizados a activos de información críticos.	Administrativas	AD.6.2	87	N/A	N/A	N/A	N/A	N/A	N/A	40	MAYOR	60	MAYOR
R43	n/a	1) Se realizan pruebas y ventanas de mantenimiento (simulacro), para determinar la efectividad de los planes de respuesta de incidentes, es 60. 2) Si La Entidad aprende continuamente sobre los incidentes de seguridad presentados, es 80.	Tecnicas	T.7.1.6	40	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R44	n/a	Se realizan pruebas a las aplicaciones o software desarrollado “in house” para determinar que umplen con los requisitos de seguridad y privacidad de la información	Tecnicas	T.6.2.8	n/a	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR
R45	n/a	Registro de actividades en seguridad (bitácora operativa).	Tecnicas	T.4.4.1	60	N/A	N/A	N/A	N/A	N/A	N/A	60	CUMPLE	80	MENOR
R46	n/a	1) Elaboración de planes de mejora es 60 2) Se implementan las acciones correctivas y planes de mejora es 80	PHVA	M.2	20	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR

R47	n/a	1) Si los planes de respuesta a incidentes incluyen algunas áreas de la entidad y si se evalúa la efectividad los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro es 60 2) Se incluyen todas las áreas de la Entidad, en los planes de respuesta de incidentes es 80	Tecnicas	T.7.1.5	40	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R48	n/a	Gestión de acceso de usuario.	Tecnicas	T.1.2	83	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR
R49	n/a	Control de acceso a sistemas y aplicaciones	Tecnicas	T.1.4	87	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR
R50	n/a	Controles Criptográficos	Tecnicas	T.2.1	20	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R51	n/a	Consideraciones de las auditorías de los sistemas de información.	Tecnicas	T.4.4	55	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R52	n/a	Seguridad en la operativa, registro de actividad y supervisión.	Tecnicas	T.4.7	n/a	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR
R53	n/a	Cumplimiento de los requisitos legales y contractuales.	Administrativas	AD.6.1	90	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR
EZ GESTIONADO CUANTITATIVAMENTE					495	0		0		0		660	MENOR	880	MENOR
R55	n/a	Verificación, revisión y evaluación de la continuidad de la seguridad de la informac	Administrativas	AD.5.1.3	40	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR
LIMITE DE MADUREZ OPTIMIZADO					990									1660	MENOR

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	FTIC-LP-09-15 INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA HOJA LEVANTAMIENTO DE INFORMACIÓN FUNDACIÓN GILBERTO ALZATE AVENDAÑO	

FUNCIÓN NIST	*SUBCATEGORIA NIST*	*CONTROL ANEXO A ISO 27001*	*CARGO*	*REQUISITO*	*HOJA*	*CALIFICACIÓN*	*FUNCION CSF*
DETECTAR	DE.AE-1, DE.AE-3, DE.AE-4, DE.AE-5	n/a	Responsable de SI	La detección de actividades anómalas se realiza oportunamente y se entiende el impacto potencial de los eventos: 1) Se establece y gestiona una linea base de las operaciones de red, los flujos de datos esperados para usuarios y sistemas. 2) Se agregan y correlacionan datos de eventso de multiples fuentes y sensores. 3) Se determina el impacto de los eventos 4) Se han establecido los umbrales de alerta de los incidentes.	n/a	40	DETECTAR
DETECTAR	DE.AE-1	n/a	Responsable de SI	La efectividad de las tecnologías de protección se comparte con las partes autorizadas y apropiadas.	n/a	20	DETECTAR
IDENTIFICAR	ID.BE-2	n/a	Responsable de SI	La entidad conoce su papel dentro del estado Colombiano, identifica y comunica a las partes interesadas la infraestructura crítica.	n/a	80	IDENTIFICAR
IDENTIFICAR	ID.GV-4	n/a	Responsable de SI	La gestión de riesgos tiene en cuenta los riesgos de ciberseguridad	n/a	0	IDENTIFICAR
RESPONDER	RS.CO-4, RS.CO-5	n/a	Responsable de SI	Las actividades de respuesta son coordinadas con las partes interesadas tanto internas como externas, segun sea apropiado, para incluir soporte externo de entidades o agencias estatales o legales.: 1) Los planes de respuesta a incidentes estan coordinados con las partes interesadas de manera consistente. 2) De manera voluntaria se comparte información con partes interesadas externas para alcanzar una conciencia más amplia de la situación de ciberseguridad.	n/a	80	RESPONDER
RECUPERAR	RC.CO-1, RC.CO-2, RC.CO-3	n/a	Responsable de SI	Las actividades de restauración son coordinadas con las partes internas y externas, como los centros de coordinación, provedores de servicios de Internet, los dueños de los sistemas atacados, las víctimas, otros CSIRT, y proveedores.: 1) Se gestionan las comunicaciones hacia el público. 2) Se procura la no afectación de la reputación o la reparación de la misma. 3) Las actividasdes de recuperación son comunicadas a las partes interesadas internas y a los grupos de gerentes y directores.	n/a	80	RECUPERAR
IDENTIFICAR	ID.RA-3	n/a	Responsable de SI	Las amenazas internas y externas son identificadas y documentadas.	n/a	80	IDENTIFICAR
RESPONDER	RS.IM-2	n/a	Responsable de SI	Las estrategias de respuesta se actualizan	n/a	40	RESPONDER
IDENTIFICAR	ID.BE-3	n/a	Responsable de SI	Las prioridades relaciondadas con la misión, objetivos y actividades de la Entidad son establecidas y comunicadas.	n/a	100	IDENTIFICAR
IDENTIFICAR	ID.RA-4	n/a	Responsable de SI	Los impactos potenciales en la entidad y su probabilidad son identificados	n/a	60	IDENTIFICAR
RECUPERAR	RC.IM-1, RC.IM-2	n/a	Responsable de SI	Los planes de recuperación y los procesos son mejorados incorporando las lecciones aprendidas para actividades futuras: 1) Los planes de recuperación incorporan las lecciones aprendidas. 2) Las estrategias de recuperación son actualizadas.	n/a	60	RECUPERAR
PROTEGER	PR.IP-7	n/a	Responsable de SI	Los procesos de protección son continuamente mejorados	n/a	60	PROTEGER
DETECTAR	DE.CM-1, DE.CM-2, DE.CM-7	n/a	Responsable de SI	Los sistemas de información y los activos son monitoreados a intervalos discretos para identificar los eventos de ciberseguridad y verificar la efectividad de las medidas de protección: 1) La red es monitoreada para detectar eventos potenciales de ciberseguridad. 2) El ambiente físico es monitoreados para detectar eventos potenciales de ciberseguridad. 3) Se monitorea en busqueda de eventos como personal no autorizado, u otros eventos relacionados con conecciones, dispositivos y software.	n/a	60	DETECTAR
IDENTIFICAR	ID.GV-1	A.5.1.1	n/a	n/a	Administrativas	60	IDENTIFICAR
IDENTIFICAR	ID.AM-6	A.6.1.1	n/a	n/a	Administrativas	20	IDENTIFICAR
IDENTIFICAR	ID.GV-2	A.6.1.1	n/a	n/a	Administrativas	20	IDENTIFICAR
PROTEGER	PR.AT-2	A.6.1.1	n/a	n/a	Administrativas	20	PROTEGER
PROTEGER	PR.AT-3	A.6.1.1	n/a	n/a	Administrativas	20	PROTEGER
PROTEGER	PR.AT-4	A.6.1.1	n/a	n/a	Administrativas	20	PROTEGER
PROTEGER	PR.AT-5	A.6.1.1	n/a	n/a	Administrativas	20	PROTEGER
DETECTAR	DE.DP-1	A.6.1.1	n/a	n/a	Administrativas	20	DETECTAR
RESPONDER	RS.CO-1	A.6.1.1	n/a	n/a	Administrativas	20	RESPONDER
PROTEGER	PR.AC-4	A.6.1.2	n/a	n/a	Administrativas	100	PROTEGER
PROTEGER	PR.DS-5	A.6.1.2	n/a	n/a	Administrativas	100	PROTEGER
RESPONDER	RS.CO-3	A.6.1.2	n/a	n/a	Administrativas	100	RESPONDER
RESPONDER	RS.CO-2	A.6.1.3	n/a	n/a	Administrativas	100	RESPONDER
IDENTIFICAR	ID.RA-2	A.6.1.4	n/a	n/a	Administrativas	100	IDENTIFICAR
PROTEGER	PR.IP-2	A.6.1.5	n/a	n/a	Administrativas	100	PROTEGER
PROTEGER	PR.AC-3	A.6.2.2	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.DS-5	A.7.1.1	n/a	n/a	Administrativas	80	PROTEGER
PROTEGER	PR.IP-11	A.7.1.1	n/a	n/a	Administrativas	80	PROTEGER
PROTEGER	PR.DS-5	A.7.1.2	n/a	n/a	Administrativas	80	PROTEGER
IDENTIFICAR	ID.GV-2	A.7.2.1	n/a	n/a	Administrativas	40	IDENTIFICAR
PROTEGER	PR.AT-1	A.7.2.2	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.AT-2	A.7.2.2	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.AT-3	A.7.2.2	n/a	n/a	Administrativas	60	PROTEGER

PROTEGER	PR.AT-4	A.7.2.2	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.AT-5	A.7.2.2	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.DS-5	A.7.3.1	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.IP-11	A.7.3.1	n/a	n/a	Administrativas	40	PROTEGER
IDENTIFICAR	ID AM-1	A.8.1.1	n/a	n/a	Administrativas	60	IDENTIFICAR
IDENTIFICAR	ID AM-2	A.8.1.1	n/a	n/a	Administrativas	60	IDENTIFICAR
IDENTIFICAR	ID.AM-5	A.8.1.1	n/a	n/a	Administrativas	60	IDENTIFICAR
IDENTIFICAR	ID AM-1	A.8.1.2	n/a	n/a	Administrativas	100	IDENTIFICAR
IDENTIFICAR	ID AM-2	A.8.1.2	n/a	n/a	Administrativas	100	IDENTIFICAR
PROTEGER	PR.IP-11	A.8.1.4	n/a	n/a	Administrativas	100	PROTEGER
PROTEGER	PR.DS-5	A.8.2.2	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.PT-2	A.8.2.2	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.DS-1	A.8.2.3	n/a	n/a	Administrativas	80	PROTEGER
PROTEGER	PR.DS-2	A.8.2.3	n/a	n/a	Administrativas	80	PROTEGER
PROTEGER	PR.DS-3	A.8.2.3	n/a	n/a	Administrativas	80	PROTEGER
PROTEGER	PR.DS-5	A.8.2.3	n/a	n/a	Administrativas	80	PROTEGER
PROTEGER	PR.IP-6	A.8.2.3	n/a	n/a	Administrativas	80	PROTEGER
PROTEGER	PR.PT-2	A.8.2.3	n/a	n/a	Administrativas	80	PROTEGER
PROTEGER	PR.DS-3	A.8.3.1	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.IP-6	A.8.3.1	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.PT-2	A.8.3.1	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.DS-3	A.8.3.2	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.IP-6	A.8.3.2	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.DS-3	A.8.3.3	n/a	n/a	Administrativas	n/a	PROTEGER
PROTEGER	PR.PT-2	A.8.3.3	n/a	n/a	Administrativas	n/a	PROTEGER
PROTEGER	PR.DS-5	A.9.1.1	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.AC-4	A.9.1.2	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.DS-5	A.9.1.2	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.PT-3	A.9.1.2	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.AC-1	A.9.2.1	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.AC-1	A.9.2.2	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.AC-4	A.9.2.3	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.DS-5	A.9.2.3	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.AC-1	A.9.2.4	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.AC-1	A.9.3.1	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.AC-4	A.9.4.1	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.DS-5	A.9.4.1	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.AC-1	A.9.4.2	n/a	n/a	Técnicas	n/a	PROTEGER
PROTEGER	PR.AC-1	A.9.4.3	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.AC-4	A.9.4.4	n/a	n/a	Técnicas	n/a	PROTEGER
PROTEGER	PR.DS-5	A.9.4.4	n/a	n/a	Técnicas	n/a	PROTEGER
PROTEGER	PR.DS-5	A.9.4.5	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.AC-2	A.11.1.1	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.AC-2	A.11.1.2	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.MA-1	A.11.1.2	n/a	n/a	Técnicas	100	PROTEGER
IDENTIFICAR	ID.BE-5	A.11.1.4	n/a	n/a	Técnicas	40	IDENTIFICAR
PROTEGER	PR.AC-2	A.11.1.4	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.IP-5	A.11.1.4	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.AC-2	A.11.1.6	n/a	n/a	Técnicas	n/a	PROTEGER
PROTEGER	PR.IP-5	A.11.2.1	n/a	n/a	Técnicas	80	PROTEGER
IDENTIFICAR	ID.BE-4	A.11.2.2	n/a	n/a	Técnicas	80	IDENTIFICAR
PROTEGER	PR.IP-5	A.11.2.2	n/a	n/a	Técnicas	80	PROTEGER
IDENTIFICAR	ID.BE-4	A.11.2.3	n/a	n/a	Técnicas	80	IDENTIFICAR
PROTEGER	PR.AC-2	A.11.2.3	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.IP-5	A.11.2.3	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.MA-1	A.11.2.4	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.MA-2	A.11.2.4	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.MA-1	A.11.2.5	n/a	n/a	Técnicas	80	PROTEGER
IDENTIFICAR	ID.AM-4	A.11.2.6	n/a	n/a	Técnicas	40	IDENTIFICAR
PROTEGER	PR.DS-3	A.11.2.7	n/a	n/a	Técnicas	20	PROTEGER
PROTEGER	PR.IP-6	A.11.2.7	n/a	n/a	Técnicas	20	PROTEGER
PROTEGER	PR.PT-2	A.11.2.9	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.IP-1	A.12.1.2	n/a	n/a	Técnicas	0	PROTEGER
PROTEGER	PR.IP-3	A.12.1.2	n/a	n/a	Técnicas	0	PROTEGER
IDENTIFICAR	ID.BE-4	A.12.1.3	n/a	n/a	Técnicas	40	IDENTIFICAR
PROTEGER	PR.DS-7	A.12.1.4	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-6	A.12.2.1	n/a	n/a	Técnicas	60	PROTEGER
DETECTAR	DE.CM-4	A.12.2.1	n/a	n/a	Técnicas	60	DETECTAR
RESPONDER	RS.MI-2	A.12.2.1	n/a	n/a	Técnicas	60	RESPONDER
PROTEGER	PR.DS-4	A.12.3.1	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.IP-4	A.12.3.1	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.PT-1	A.12.4.1	n/a	n/a	Técnicas	60	PROTEGER
DETECTAR	DE.CM-3	A.12.4.1	n/a	n/a	Técnicas	60	DETECTAR
RESPONDER	RS.AN-1	A.12.4.1	n/a	n/a	Técnicas	60	RESPONDER
PROTEGER	PR.PT-1	A.12.4.2	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.PT-1	A.12.4.3	n/a	n/a	Técnicas	60	PROTEGER
RESPONDER	RS.AN-1	A.12.4.3	n/a	n/a	Técnicas	60	RESPONDER
PROTEGER	PR.PT-1	A.12.4.4	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-6	A.12.5.1	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.IP-1	A.12.5.1	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.IP-3	A.12.5.1	n/a	n/a	Técnicas	60	PROTEGER
DETECTAR	DE.CM-5	A.12.5.1	n/a	n/a	Técnicas	60	DETECTAR
IDENTIFICAR	ID.RA-1	A.12.6.1	n/a	n/a	Técnicas	60	IDENTIFICAR
IDENTIFICAR	ID.RA-5	A.12.6.1	n/a	n/a	Técnicas	60	IDENTIFICAR
PROTEGER	PR.IP-12	A.12.6.1	n/a	n/a	Técnicas	60	PROTEGER
DETECTAR	DE.CM-8	A.12.6.1	n/a	n/a	Técnicas	60	DETECTAR
RESPONDER	RS.MI-3	A.12.6.1	n/a	n/a	Técnicas	60	RESPONDER
PROTEGER	PR.IP-1	A.12.6.2	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.IP-3	A.12.6.2	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.AC-3	A.13.1.1	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.AC-5	A.13.1.1	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.DS-2	A.13.1.1	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.PT-4	A.13.1.1	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.AC-5	A.13.1.3	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-5	A.13.1.3	n/a	n/a	Técnicas	40	PROTEGER
IDENTIFICAR	ID.AM-3	A.13.2.1	n/a	n/a	Técnicas	40	IDENTIFICAR
PROTEGER	PR.AC-5	A.13.2.1	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.AC-3	A.13.2.1	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-2	A.13.2.1	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-5	A.13.2.1	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.PT-4	A.13.2.1	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-2	A.13.2.3	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-5	A.13.2.3	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-5	A.13.2.4	n/a	n/a	Técnicas	60	PROTEGER

PROTEGER	PR.IP-2	A.14.1.1	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-2	A.14.1.2	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-5	A.14.1.2	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-6	A.14.1.2	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-2	A.14.1.3	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.DS-5	A.14.1.3	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.DS-6	A.14.1.3	n/a	n/a	Técnicas	80	PROTEGER
PROTEGER	PR.IP-2	A.14.2.1	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.IP-1	A.14.2.2	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.IP-3	A.14.2.2	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.IP-1	A.14.2.3	n/a	n/a	Técnicas	n/a	PROTEGER
PROTEGER	PR.IP-1	A.14.2.4	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.IP-2	A.14.2.5	n/a	n/a	Técnicas	40	PROTEGER
DETECTAR	DE.CM-6	A.14.2.7	n/a	n/a	Técnicas	60	DETECTAR
DETECTAR	DE.DP-3	A.14.2.8	n/a	n/a	Técnicas	n/a	DETECTAR
PROTEGER	PR.IP-9	A.16.1.1	n/a	n/a	Técnicas	60	PROTEGER
DETECTAR	DE.AE-2	A.16.1.1	n/a	n/a	Técnicas	60	DETECTAR
RESPONDER	RS.CO-1	A.16.1.1	n/a	n/a	Técnicas	60	RESPONDER
DETECTAR	DE.DP-4	A.16.1.2	n/a	n/a	Técnicas	40	DETECTAR
RESPONDER	RS.CO-2	A.16.1.3	n/a	n/a	Técnicas	100	RESPONDER
DETECTAR	DE.AE-2	A.16.1.4	n/a	n/a	Técnicas	n/a	DETECTAR
RESPONDER	RS.AN-4	A.16.1.4	n/a	n/a	Técnicas	n/a	RESPONDER
RESPONDER	RS.RP-1	A.16.1.5	n/a	n/a	Técnicas	40	RESPONDER
RESPONDER	RS.AN-1	A.16.1.5	n/a	n/a	Técnicas	40	RESPONDER
RESPONDER	RS.MI-2	A.16.1.5	n/a	n/a	Técnicas	40	RESPONDER
RECUPERAR	RC.RP-1	A.16.1.5	n/a	n/a	Técnicas	40	RECUPERAR
DETECTAR	DE.DP-5	A.16.1.6	n/a	n/a	Técnicas	40	DETECTAR
RESPONDER	RS.AN-2	A.16.1.6	n/a	n/a	Técnicas	40	RESPONDER
RESPONDER	RS.IM-1	A.16.1.6	n/a	n/a	Técnicas	40	RESPONDER
RESPONDER	RS.AN-3	A.16.1.7	n/a	n/a	Técnicas	n/a	RESPONDER
IDENTIFICAR	ID.BE-5	A.17.1.1	n/a	n/a	Administrativas	20	IDENTIFICAR
PROTEGER	PR.IP-9	A.17.1.1	n/a	n/a	Administrativas	20	PROTEGER
IDENTIFICAR	ID.BE-5	A.17.1.2	n/a	n/a	Administrativas	20	IDENTIFICAR
PROTEGER	PR.IP-4	A.17.1.2	n/a	n/a	Administrativas	20	PROTEGER
PROTEGER	PR.IP-9	A.17.1.2	n/a	n/a	Administrativas	20	PROTEGER
PROTEGER	PR.IP-4	A.17.1.3	n/a	n/a	Administrativas	0	PROTEGER
PROTEGER	PR.IP-10	A.17.1.3	n/a	n/a	Administrativas	0	PROTEGER
IDENTIFICAR	ID.BE-5	A.17.2.1	n/a	n/a	Administrativas	40	IDENTIFICAR
IDENTIFICAR	ID.GV-3	A.18.1	n/a	n/a	Administrativas	90	IDENTIFICAR
PROTEGER	PR.IP-4	A.18.1.3	n/a	n/a	Administrativas	80	PROTEGER
DETECTAR	DE.DP-2	A.18.1.4	n/a	n/a	Administrativas	100	DETECTAR
PROTEGER	PR.IP-12	A.18.2.2	n/a	n/a	Administrativas	100	PROTEGER
IDENTIFICAR	ID.RA-1	A.18.2.3	n/a	n/a	Administrativas	100	IDENTIFICAR
IDENTIFICAR	ID.BE-1	A.15.1	n/a	n/a	Administrativas	80	IDENTIFICAR
IDENTIFICAR	ID.BE-1	A.15.2	n/a	n/a	Administrativas	100	IDENTIFICAR
PROTEGER	PR.MA-2	A.15.1	n/a	n/a	Administrativas	80	PROTEGER
PROTEGER	PR.MA-2	A.15.2	n/a	n/a	Administrativas	100	PROTEGER
DETECTAR	DE.CM-6	A.15.2	n/a	n/a	Administrativas	100	DETECTAR