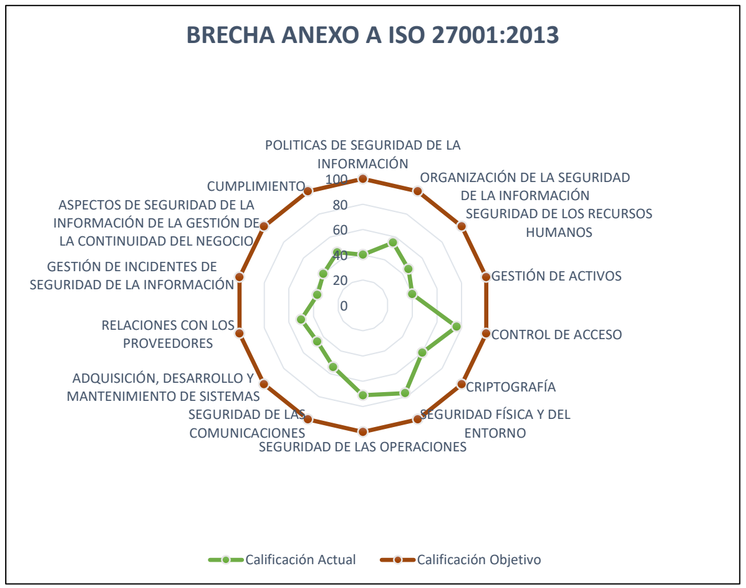
INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD HOJA PORTADA	
ENTIDAD EVALUADA	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR
FECHAS DE EVALUACIÓN	30-ene-2025
CONTACTO	WWW.ICULTUR.GOV.CO
ELABORADO POR	CONTRATISTA ICULTUR (OFICINA DE TIC)

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	40	100	**REPETIBLE**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	55	100	**EFECTIVO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	46	100	**EFECTIVO**
A.8	GESTIÓN DE ACTIVOS	40	100	**REPETIBLE**
A.9	CONTROL DE ACCESO	76	100	**GESTIONADO**
A.10	CRIPTOGRAFÍA	60	100	**EFECTIVO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	77	100	**GESTIONADO**
A.12	SEGURIDAD DE LAS OPERACIONES	71	100	**GESTIONADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	54	100	**EFECTIVO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	46	100	**EFECTIVO**
A.15	RELACIONES CON LOS PROVEEDORES	50	100	**EFECTIVO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	37	100	**REPETIBLE**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40	100	**REPETIBLE**
A.18	CUMPLIMIENTO	46,5	100	**EFECTIVO**
PROMEDIO EVALUACIÓN DE CONTROLES		**53**	**100**	EFECTIVO

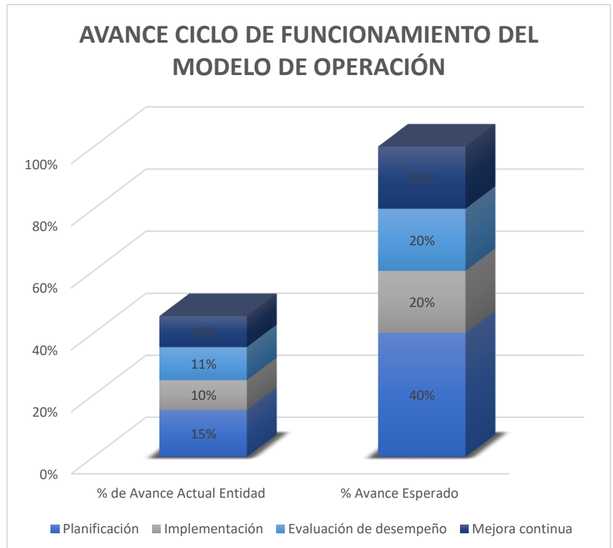


INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD HOJA PORTADA	
ENTIDAD EVALUADA	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR
FECHAS DE EVALUACIÓN	30-ene-2025
CONTACTO	WWW.ICULTUR.GOV.CO
ELABORADO POR	CONTRATISTA ICULTUR (OFICINA DE TIC)

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

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

AVANCE PHVA		
COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Planificación	15%	40%
Implementación	10%	20%
Evaluación de desempeño	11%	20%
Mejora continua	10%	20%
TOTAL	45%	100%



INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD HOJA PORTADA	
ENTIDAD EVALUADA	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR
FECHAS DE EVALUACIÓN	30-ene-2025
CONTACTO	WWW.ICULTUR.GOV.CO
ELABORADO POR	CONTRATISTA ICULTUR (OFICINA DE TIC)

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

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	SUFICIENTE
Definido	INTERMEDIO
Administrado	CRÍTICO
Optimizado	CRÍTICO

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%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD HOJA PORTADA	
ENTIDAD EVALUADA	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR
FECHAS DE EVALUACIÓN	30-ene-2025
CONTACTO	WWW.ICULTUR.GOV.CO
ELABORADO POR	CONTRATISTA ICULTUR (OFICINA DE TIC)

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

CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)

IDENTIFICAR	PROTEGER	DETECTAR	RESPONDER	RECUPERARSE
• Gestión de activos • Ambiente de negocios • Evaluación de riesgos • Estrategia de gestión de riesgos	• Control de acceso • Capacitación y sensibilización • Seguridad datos • Protección información y procedimientos • Mantenimiento • Tecnología de protección	• Anomalías y eventos • Monitoreo continuo de la seguridad • Proceso de detección	• Planes de respuesta • Comunicaciones • Análisis • Mitigación • Mejoras	• Planes de recuperación • Mejoras • Comunicaciones

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	0	100
DETECTAR	0	100
RESPONDER	0	100
RECUPERAR	0	100
PROTEGER	0	100

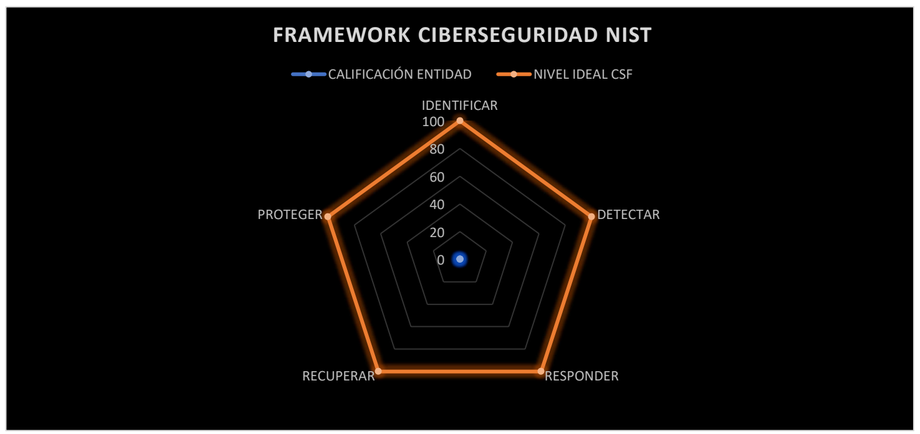


TABLA DE ESCALA DE VALORACIÓN DE CONTROLOES - ISO 27001:2013 ANEXO A

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.

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

DATOS BASICOS	
Tipo Entidad	De orden nacional
Misión	https://www.icultur.gov.co/Institucional/mision-y-vision
Analisis de Contexto	https://www.icultur.gov.co/Institucional/mision-y-vision
Mapa de Procesos	https://www.icultur.gov.co/Documentos/Transp_Desempeno_MIPG/diagrama%20de%20procesos_12_2025-03-28_120910.pdf
Organigrama	https://www.icultur.gov.co/Documentos/Transp_Instrumentos_Publica/Organigrama%20Icultur_35_2025-04-09_113102.pdf

PREGUNTAS	
Qué le preocupa a la Entidad en temas de seguridad de la	La protección de la información de los beneficiarios desde el punto de vista de la confidencialidad y la integridad.
En qué nivel de madurez considera que está?	Definido
En que componente del ciclo PHVA considera que va?	Implementación

NO.	DATOS E INFORMACIÓN A RECOLECTAR PARA LA EVALUACIÓN Lista de información BASICA a solicitar	NOMBRE DEL DOCUMENTO	OBSERVACIONES
1	Tipo de entidad (Nacional, Territorial A, Territorial B o C)	ACUERDO 535	**ENTIDAD DE ORDEN NACIONAL**
2	Misión	https://www.icultur.gov.co/Institucional/mision-y-vision	
3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que		
4	Mapa de Procesos	https://www.icultur.gov.co/Documentos/Transp_Desempeno_MIPG/diagrama%20de%20procesos_12_2025-03-28_120910.pdf	
5	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces	cumentos/Transp_Instrumentos_Publica/Organigrama%20Ic	
6	Políticas de seguridad de la información formalizada y firmada	https://www.icultur.gov.co/Documentos/Transp_Desempeno_MIPG/%20acta%20de%20comite_1	
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	Políticas de seguridad de la información	
8	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e		
9	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado,		
10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección		
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)	https://www.icultur.gov.co/Documentos/Transp_Planeacion/Plan%20estrategico%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informacion%202024__2025-04-10_090546.pdf	
12	Procedimientos de control documental del MSPI	https://www.icultur.gov.co/Documentos/Transp_Planeacion/Modelo%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informacion%202024__2025-04-08_113755.pdf	
13	Metodología de Gestión de riesgos		
14	Riesgos identificados y valorados de acuerdo a la metodología		
15	Planes de tratamiento de los riesgos	https://www.icultur.gov.co/Documentos/Transp_Planeacion/Plan%20estrategico%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informacion%202024__2025-04-10_090546.pdf	
16	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la		
17	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad		
18	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta		
19	Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información		
20	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección		
21	Inventario de áreas de procesamiento de información y telecomunicaciones		
22	Diagrama de red de alto nivel o arquitectura de TI	PETI	
23	Inclusión de la seguridad de la información en la gestión de proyectos		
24	Inventario de partes externas o terceros a los que se transfiere información de la entidad		
25	Formato de acuerdo de transferencia de información		
26	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden		
27	Reporte de eventos e incidentes de seguridad de la información de los últimos 12 meses.	N/A	
28	Plan de continuidad de la Entidad aprobado		
29	Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información		
30	Listado de auditorias relacionadas con seguridad de la información realizadas en la entidad		
31	Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno en Línea.	https://www.icultur.gov.co/Transparencia/Planeacion	
32	Indicadores y métricas de seguridad de la información definidos.		
33	Declaración de aplicabilidad		
34	Aceptación de los riesgos residuales por parte de los dueños de los riesgos		

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR			
	Lista de información para aquellas entidades que hayan avanzado en la fase de IMPLEMENTACIÓN		
35	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	https://www.icultur.gov.co/Documentos/Transp_Planeacion/Plan%20estrategico%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informacion%202024__2025-04-10_090546.pdf	
36	Avance en la ejecución del plan de tratamiento de riesgos	https://www.icultur.gov.co/Documentos/Transp_Planeacion/Plan%20estrategico%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informacion%202024__2025-04-10_090546.pdf	
37	Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.		
	Lista de información para aquellas entidades que hayan avanzado en la fase de EVALUACIÓN DE DESEMPEÑO		
38	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.		
39	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.	https://www.icultur.gov.co/Transparencia/control-interno	
40	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.		
	Lista de información para aquellas entidades que hayan avanzado en la fase de MEJORA CONTINUA		
41	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.		
42	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta		

	Porcentaje de cumplimiento del MSPI en los procesos de la entidad	**# total de procesos**	**# de procesos definidos en el alcance**	**Total avance por procesos**
43	Con base al alcance definido en la política de seguridad y el total de	13	6	46%

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD
HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR		
RESPONSABLE / ÁREA	**TEMA**	**FUNCIONARIO**
Control interno	Revisiones de seguridad de la información	JOSE CUERO
	Revisión independiente de la seguridad de la información	
	Cumplimiento con las políticas y normas de seguridad.	
	CUMPLIMIENTO	
	Auditoría Interna Plan	
	Auditoría Interna Ejecución y Subsanación de hallazgos y brechas	
Gestión humana	Selección e investigación de antecedentes	VANEZA DAGUER
	Términos y condiciones del empleo	
Líder de Proceso 1	**Promoción y fomento deportivos**	VANEZA DAGUER
	DESCRIPCIÓN DEL PROCESO	
Líder de Proceso 2	**Promoción y fomento de la actividad física, la recreación y el uso del tiempo libre**	VANEZA DAGUER
	DESCRIPCIÓN DEL PROCESO	
Líder de Proceso 3	**Gestión de la Infraestructura**	VANEZA DAGUER
	DESCRIPCIÓN DEL PROCESO	
Responsable de compras y adquisiciones	RELACIONES CON LOS PROVEEDORES	VANEZA DAGUER Directora Administrativa y Financiera
	Seguridad de la información en las relaciones con los proveedores	
	Gestión de la prestación de servicios de proveedores	

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD
HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR		
RESPONSABLE / ÁREA	**TEMA**	**FUNCIONARIO**
Responsable de la continuidad	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Directora Administrativa y Financiera RUBEN MIRANDA Jefe de Contabilidad MARIO IMBETT Sistemas
	Continuidad de la seguridad de la información	
	Planificación de la continuidad de la seguridad de la información	
	Implementación de la continuidad de la seguridad de la información	
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
	Redundancias	
	Disponibilidad de instalaciones de procesamiento de información	
Responsable de la seguridad física	SEGURIDAD FÍSICA Y DEL ENTORNO	Directora Administrativa y Financiera
	ÁREAS SEGURAS	
	Perímetro de seguridad física	
	Áreas de despacho y carga	
	Visita al Centro de Cómputo	MARIO IMBETT
	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
	SEGURIDAD DE LOS RECURSOS HUMANOS	
	Antes de asumir el empleo	
	Durante la ejecución del empleo	
	Terminación y cambio de empleo	
	GESTIÓN DE ACTIVOS	
	CUMPLIMIENTO	
	Cumplimiento de requisitos legales y contractuales	
	CONTROL DE ACCESO	
	CRIPTOGRAFÍA	
	SEGURIDAD FÍSICA Y DEL ENTORNO	
	SEGURIDAD DE LAS OPERACIONES	
	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	
	Procedimientos de operación documentados	
	Gestión de cambios	

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD
HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR		
RESPONSABLE / ÁREA	**TEMA**	**FUNCIONARIO**
Responsable de SI	Gestión de capacidad	JEFES DE AREA OFICINAS: Oficina Juridica Oficina de Insfraestructura Oficina de Planeacion Direccion Administrativa y Financiera Oficina de Sistemas Oficina de Archivo Oficina de Talento Humano Oficina de Contabilidad
	Separación de los ambientes de desarrollo, pruebas y operación	
	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	
	COPIAS DE RESPALDO	
	REGISTRO Y SEGUIMIENTO	
	Registro de eventos	
	Protección de la información de registro	
	Registros del administrador y del operador	
	Sincronización de relojes	
	CONTROL DE SOFTWARE OPERACIONAL	
	Instalación de software en sistemas operativos	
	GESTIÓN DE LA VULNERABILIDAD TÉCNICA	
	Gestión de las vulnerabilidades técnicas	
	Restricciones sobre la instalación de software	
	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	
	Controles sobre auditorías de sistemas de información	
	SEGURIDAD DE LAS COMUNICACIONES	
	GESTIÓN DE LA SEGURIDAD DE LAS REDES	
	TRANSFERENCIA DE INFORMACIÓN	
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	
	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	
	DATOS DE PRUEBA	
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
	Alcande MSPI (Modelo de Seguridad y Privacidad de la Información)	
	Identificación y valoración de riesgos	
	Tratamiento de riesgos de seguridad de la información	

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD
HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR		
RESPONSABLE / ÁREA	**TEMA**	**FUNCIONARIO**
	Toma de conciencia, educación y formación en la seguridad de la información	
	Planificación y control operacional	
	Implementación del plan de tratamiento de riesgos	
	Indicadores de gestión del MSPI	
	Plan de seguimiento, evaluación y análisis del MSPI	
	Evaluación del plan de tratamiento de riesgos	
	Plan de seguimiento, evaluación y análisis del MSPI	
	Tratamiento de temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, o en los comités directivos interdisciplinarios de la Entidad	
	Con base en el inventario de activos de información clasificado, se establece la caracterización de cada uno de los sistemas de información.	
	La entidad conoce su papel dentro del estado Colombiano, identifica y comunica a las partes interesadas la infraestructura crítica.	
	Las prioridades relaciondadas con la misión, objetivos y actividades de la Entidad son establecidas y comunicadas.	
	La gestión de riesgos tiene en cuenta los riesgos de ciberseguridad	
	Detección de actividades anómalas	
	Respuesta a incidentes de ciberseguridad, planes de recuperación y restauración	
	Teletrabajo	
	Manejo de medios	
	Derechos de propiedad intelectual.	
	CONTROL DE ACCESO	
	SEGURIDAD DE LAS OPERACIONES	
	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD
HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR		
RESPONSABLE / ÁREA	**TEMA**	**FUNCIONARIO**
Responsable de TICs	COPIAS DE RESPALDO	Oficina Sistemas y Equipo de Trabajo
	CONTROL DE SOFTWARE OPERACIONAL	
	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	
	SEGURIDAD DE LAS COMUNICACIONES	
	GESTIÓN DE LA SEGURIDAD DE LAS REDES	
	TRANSFERENCIA DE INFORMACIÓN	
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
	Plan y Estrategia de transisicón de IPv4 a IPv6	
	Implementación del plan de estrategia de transición de IPv4 a IPv6	
	Redundancias	
Calidad	Procedimientos de control documental del MSPI	

INSTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TECNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

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**					**40**	
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			40	
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**						**55**	
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**					**40**	
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 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			40	
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 auditoría y la supervisión de cargos superiores.			40	
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.			40	

INSTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TECNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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.			40	
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 de instalaciones y otros procesos de soporte.	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 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 proyecto, para identificar los controles necesarios; c) Que la seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.			40	
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			60	

INSTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TECNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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; e) el uso de redes domésticas y requisitos o			80	
SEGURIDAD DE LOS RECURSOS HUMANOS											
AD.3	**Responsable de SI/Gestión Humana/Líderes de los procesos**	**SEGURIDAD DE LOS RECURSOS HUMANOS**		**A.7**						**46**	
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**					**30**	
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 ejemplo, información financiera o información muy confidencial, la organización debería también considerar verificaciones adicionales más detalladas (por ejemplo estudio de seguridad, polígrafo, visita domiciliaria) g) También se debería asegurar un proceso de selección para contratistas. En estos casos, el			40	
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				20	
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**					**47**	

INSTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TECNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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. e) Cuenten con un canal para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información (“denuncias internas”).			40	
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 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.			60	
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 seguridad de la información.	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?			40	
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**					**60**	
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.			60	
GESTIÓN DE ACTIVOS											
AD.4	**Responsable de SI**	**GESTIÓN DE ACTIVOS**		**A.8**						**40**	
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**					**45**	

INSTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TECNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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			40	
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.			40	
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.			40	
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 período 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.			60	
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**						**47**	

INSTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TECNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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 evalué: 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 evalué que se aplican las políticas y procedimientos de clasificación definidos. Evalué si los procesos seleccionados aplican de manera consistente estas políticas y procedimientos.			40	
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			40	
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.			60	
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**						**27**	
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 auditoria; 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)			40	

INSTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TECNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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.			0	
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: a) El uso de un transporte o servicios de mensajería confiables. b) Procedimientos para verificar la identificación de los servicios de mensajería. c) Indague y evidencie como es el embalaje el cual debe proteger el contenido contra cualquier daño físico que pudiera presentarse durante el tránsito, y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protección contra cualquier factor ambiental que pueda reducir la eficacia de la restauración del medio, tal como exposición al calor, humedad o campos electromagnéticos; d) Solicite los registros que dejen evidencia del transporte donde se identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.			40	
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**						**40**	
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**						**40**	
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:** 1) Si existen planes de continuidad del negocio que contemplen los procesos críticos de la Entidad que garanticen la continuidad de los mismos. Se			40	

INSTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TECNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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.			40	
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.			40	
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	Disponibilidad 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.			40	
CUMPLIMIENTO											
AD.6	**Responsable de SI/Responsable de TICs/Control Interno**	**CUMPLIMIENTO**		**A.18**						**46,5**	
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.**			**40**	
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.			60	

INSTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TECNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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.			60	
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.			0	
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.			40	
AD.6.1.5	n/a	Reglamentación de controles criptográficos.		A.18.1.5			n/a			n/a	
AD.6.2	**Control interno**	**Revisiones de seguridad de la información**		**A.18.2**	**Modelo de Madurez Gestionado Cuantitativamente**					**53**	
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 2015 2) El resultado de las auditorías del año 2015 3) Las oportunidades de mejora o cambios en la seguridad de la información identificados.			40	
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			60	

INSTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TECNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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.			60	
RELACIONES CON LOS PROVEEDORES											
AD.7	**Responsable de compras y adquisiciones**	**RELACIONES CON LOS PROVEEDORES**		**A.15**						**50**	
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 proporcionar las instalaciones y se deben manejar los riesgos asociados a este tercero con el cual la entidad no tiene una relación comercial directa. Solicite que le indiquen como identifican para cada proveedor su cadena de suministro y obtenga evidencia de este hecho.			60	
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)			40	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

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**					**76**	
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					**80**	
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; f) la separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso); g) los requisitos para la autorización formal de las solicitudes de acceso; h) los requisitos para la revisión periódica de los derechos de acceso; i) el retiro de los derechos de acceso; j) el ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de identificación			100	
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.			60	
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					**50**	
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.			100	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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.			40	
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 con la política de control de acceso; c) mantener un proceso de autorización y un registro de todos los privilegios asignados. Sólo se debe suministrar derechos de acceso cuando el proceso de autorización esté completo; d) definir los requisitos para la expiración de los derechos de acceso privilegiado; e) establecer los derechos de acceso privilegiado a través de una identificación de usuario diferente de la usada para las actividades regulares del negocio. Las actividades regulares del negocio no se ejecutan desde una identificación privilegiada; f) tener las competencias de los usuarios con derechos de			40	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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; d) definir que la información de autenticación secreta temporal se suministra a los usuarios de una manera segura; y se evitar utilizar partes externas o de mensajes de correo electrónico no protegidos (texto claro); e) establecer que la información de autenticación secreta temporal es única para un individuo y no es fácil de adivinar; f) definir que los usuarios deben acusar recibo de la información de autenticación secreta;			40	
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.			40	
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.			40	
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					**100**	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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 secreta.	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 pueda almacenar en forma segura y que el método de almacenamiento haya sido aprobado (una bóveda para contraseñas); c) cambiar la información de autenticación secreta siempre que haya cualquier indicio de que se pueda comprometer la información; d) definir que cuando se usa contraseñas como información de autenticación secreta, se debe seleccionar contraseñas seguras con una longitud mínima suficiente que: 1) sean fáciles de recordar; 2) no estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.); 3) no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios); 4) estén libres de caracteres completamente numéricos o			100	
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					**72**	
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.			100	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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 no debe indicar qué parte de los datos es correcta o incorrecta; e) proteger contra intentos de ingreso mediante fuerza bruta; f) llevar un registro con los intentos exitosos y fallidos; g) declarar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de ingreso; h) visualizar la siguiente información al terminar un ingreso seguro: 1) registrar la fecha y la hora del ingreso previo exitoso; 2) registrar los detalles de cualquier intento de ingreso no exitoso desde el último ingreso exitoso; i) no visualizar una contraseña que se esté ingresando; j) no transmitir contraseñas en un texto claro en una red;			100	
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.			20	
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-4 PR.DS-5	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; d) autorizar el uso adhoc de programas utilitarios; e) limitar la disponibilidad de los programas utilitarios; f) registrar el uso de los programas utilitarios; g) definir y documentar los niveles de autorización para los programas utilitarios; h) retirar o deshabilitar todos los programas utilitarios innecesarios; i) No poner a disposición los programas utilitarios a los usuarios que tengan acceso a aplicaciones en sistemas en donde se requiera la separación de deberes.			40	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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.DS-5	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.			100	
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**						**60**	
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					**60**	
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 caso de llaves perdidas, llaves cuya seguridad está comprometida, o que están dañadas; e) establecer roles y responsabilidades, quién es responsable por: 1) la implementación de la política. 2) la gestión de llaves, incluida la generación de llaves; f) establecer las normas que se van a adoptar para la implementación efectiva en toda la organización (procesos del negocio);			100	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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 de vida.	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; c) distribuir llaves a las entidades previstas, incluyendo la forma de recibir y activar las llaves; d) almacenar las llaves, incluyendo la forma en que los usuarios autorizados obtienen acceso a ellas; e) cambiar o actualizar las llaves, incluyendo las reglas sobre cuándo se deben cambiar y cómo hacerlo; f) dar tratamiento a las llaves cuya seguridad está comprometida; g) revocar las llaves, incluyendo la forma de retirarlas o desactivarlas, cuando la seguridad de las llaves ha estado comprometida, o cuando un usuario deja la organización; h) recuperar las llaves que estén perdidas o dañadas; i) hacer copias de respaldo de las llaves o archivarlas; j) destruir las llaves; k) registrar y auditar las actividades relacionadas con gestión de llaves.			20	
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**						77	
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					**80**	
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 protección externa para ventanas, particularmente al nivel del suelo; c) definir un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación; el acceso a los sitios y edificaciones debe estar restringido únicamente para personal autorizado; d) establecer cuando sea aplicable y construir barreras físicas para impedir el acceso físico no autorizado y la contaminación ambiental;			100	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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 un mecanismo de autenticación de dos factores, tales como una tarjeta de acceso y un PIN secreto); c) mantener y hacer seguimiento de un libro de registro (physical log book) físico o un rastro de auditoría electrónica de todos los accesos; d) definir que todos los empleados, contratistas y partes externas deben portar algún tipo de identificación visible, y			40	
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.			40	
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.			100	
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; c) establecer que las áreas seguras vacías deben estar cerradas con llave y se revisan periódicamente; d) no se permite el ingreso y uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.			100	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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			100	
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					**73**	
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 requerida; e) establecer los controles para minimizar el riesgo de amenazas físicas y ambientales, (robo, incendio, explosivos, humo, agua (o falla en el suministro de agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo); f) establecer directrices acerca de comer, consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información; g) hacer seguimiento de las condiciones ambientales tales como temperatura y humedad, para determinar las			40	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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.			60	
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			100	
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.			100	
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			60	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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 determinar mediante una valoración de riesgos y se deben aplicar los controles adecuados según sean apropiados, (gabinetes de archivo con llave, política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina); d) establecer que cuando el equipo que se encuentra afuera de las instalaciones es transferido entre diferentes individuos y partes externas, llevar un registro que defina la cadena de custodia para el equipo, que incluya al menos los nombres y las organizaciones de los responsables del equipo.			100	
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.			100	
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).			100	
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.			0	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
SEGURIDAD DE LAS OPERACIONES											
T.4	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS OPERACIONES**		**A.12**						71	
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					**85**	
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;			100	
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 de la información.	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; e) Verificar que se han cumplido los requisitos de seguridad de la información; f) Comunicar todos los detalles de los cambios a todas las personas pertinentes; g) Tener un procedimiento de apoyo, incluidos procedimientos y responsabilidades para abortar cambios no exitosos y recuperarse de ellos, y eventos no previstos; h) Contar con un suministro de un proceso de cambio de emergencia que posibilite la implementación rápida y controlada de los cambios necesarios para resolver un incidente.			100	
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 (por ejemplo, video en tiempo real).			100	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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 a los sistemas operacionales; d) definir que solo en circunstancias excepcionales, las pruebas no se deben llevar a cabo en los sistemas operacionales; e) establecer que los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no debe ser accesibles desde sistemas operacionales cuando no se requiere; f) establecer que los usuarios deben usar diferentes perfiles de usuario para sistemas operacionales y de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error; g) definir que los datos sensibles no se debe copiar en el ambiente del sistema de pruebas, a menos que se			40	
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**						**100**	
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			100	
T.4.3	**Responsable de TICs**	**COPIAS DE RESPALDO**	**Proteger contra la pérdida de datos.**	**A.12.3**	Modelo de madurez gestionado					**100**	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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; d) establecer la información de respaldo y un nivel apropiado de protección física y del entorno, de coherencia con las normas aplicadas en el sitio principal; e) definir los medios de respaldo se debe poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso necesario; esto se debería combinar con una prueba de los procedimientos de restauración, y se debe verificar contra el tiempo de restauración requerido. f) definir las situaciones en las que la confidencialidad tiene importancia, las copias de respaldo deben estar protegidas			100	
T.4.4	Responsable de SI	**REGISTRO Y SEGUIMIENTO**	**Registrar eventos y generar evidencia.**	**A.12.4**	Modelo de madurez gestionado cuantitativamente					**45**	
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; i) establecer el uso de utilitarios y aplicaciones del sistema; j) definir los archivos a los que se tuvo acceso, y el tipo de acceso; k) establecer las direcciones y protocolos de red; l) definir las alarmas accionadas por el sistema de control de acceso; m) activar y desactivar los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión; n) registrar las transacciones ejecutadas por los usuarios en			40	
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.			60	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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.			40	
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.			40	
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;			60	
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					**50**	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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, y tomar las medidas apropiadas para tratar el riesgo asociado.	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; c) una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes potencialmente; d) establecer que una vez que se haya identificado una vulnerabilidad técnica potencial, la organización debería identificar los riesgos asociados y las acciones por tomar; esta acción puede involucrar la colocación de parches de sistemas vulnerables o la aplicación de otros controles; Si no es posible colocar controles se deben documentar en los riesgos de acuerdo a su probabilidad e impacto y colocarlo como riesgo aceptado. e) definir dependiendo de la urgencia con la que se necesite			60	
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.			40	
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					**60**	
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 auditorías 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.			60	
SEGURIDAD DE LAS COMUNICACIONES											
T.5	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS COMUNICACIONES**		**A.13**						54	
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**	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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 asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información; f) establecer los sistemas en la red que se autenticar; g) restringir la conexión de los sistemas a la red.			60	
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.			60	
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.			40	
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					**55**	
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; c) definir los procedimientos para proteger información electrónica sensible comunicada que están como adjuntos; d) establecer la política o directrices que presentan el uso aceptable de las instalaciones de comunicación; e) definir las responsabilidades del personal, las partes externas y cualquier otro usuario no comprometen a la organización, (por difamación, acoso, suplantación, envío de cadenas, compras no autorizadas, etc.); f) establecer el uso de técnicas criptográficas, (proteger la confidencialidad, la integridad y la autenticidad de la información). g) establecer las directrices sobre retención y disposición para toda la correspondencia del negocio, incluidos mensajes, de acuerdo con la legislación y reglamentaciones locales y			60	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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 etiqueta se entiende de inmediato, y que la información está protegida apropiadamente; h) definir las normas técnicas para registro y lectura de información y software; i) cualquier control especial que se requiera para proteger elementos críticos, tales como criptografía; j) mantener una cadena de custodia para la información mientras está en tránsito;			40	
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.			60	
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			60	
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS											

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
T.6	**Responsable de SI/Responsable de TICs**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		**A.14**						46	
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					**30**	
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; e) definir los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso y seguimiento, y de no repudio; f) establecer los requisitos exigidos por otros controles de seguridad, (interfaces con el ingreso o seguimiento, o los sistemas de detección de fuga de datos).			0	
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; d) determinar y cumplir los requisitos para confidencialidad, integridad, prueba de despacho y recibo de documentos clave y el no repudio de los contratos, (asociados con procesos de ofertas y contratos); e) definir el nivel de confianza requerido en la integridad de los documentos clave; f) establecer los requisitos de protección de cualquier información confidencial; g) definir la confidencialidad e integridad de cualquier transacción de pedidos, información de pagos, detalles de la dirección de entrega y confirmación de recibos;			60	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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 una plataforma de almacenamiento existente en la intranet de la organización, y no retenido ni expuesto en un medio de almacenamiento accesible directamente desde Internet); f) utilizar una autoridad confiable (para los propósitos de emitir y mantener firmas digitales o certificados digitales), la			60	
T.6.2	**Responsable de SI**	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE**	**Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.**	**A.14.2**	Modelo de madurez definido					**47**	
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; d) definir los puntos de chequeo de seguridad dentro de los hitos del proyecto; e) establecer los depósitos seguros; f) definir la seguridad en el control de la versión; g) establecer el conocimiento requerido sobre seguridad de la aplicación; h) definir la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.			60	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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; g) revisar antes de la implementación, asegurar que los usuarios autorizados aceptan los cambios; h) asegurar que el conjunto de documentación del sistema está actualizado al completar cada cambio, y que la documentación antigua se lleva al archivo permanente, o se dispone de ella; i) mantener un control de versiones para todas las actualizaciones de software; j) mantener un rastro de auditoría de todas las solicitudes de			40	
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.			60	
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.			40	
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.			40	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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.			40	
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; g) definir la evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas; h) definir los certificados de depósito de títulos en garantía; (el código fuente ya no está disponible); i) establecer el derecho contractual con relación a procesos y			40	
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.			60	
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.			40	
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					**60**	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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.			60	
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**						37	
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**						**37**	
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; b) establecer los procedimientos para asegurar que: 1) el personal competente maneje las cuestiones relacionadas con incidentes de seguridad de la información dentro de la			0	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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.			60	
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 seguridad de la información observada o sospechada en los sistemas o servicios.	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.			0	
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.			40	
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; e) asegurar que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior; f) comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo; g) tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente; g) establecer que una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto. h) de acuerdo a la NIST se deben investigar las notificaciones			60	

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
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.			40	
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.			60	

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

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 consideraró: 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			40	
	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			40 40	0 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			40	

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

COMPONENTE	ID	CARGO	ITEM	DESCRIPCIÓN	PRUEBA	CIBERSEGURIDAD	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO PHVA	RECOMENDACIÓN
PLANIFICACIÓN	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			40	0
	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			40	0
	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			60	

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

COMPONENTE	ID	CARGO	ITEM	DESCRIPCIÓN	PRUEBA	CIBERSEGURIDAD	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO PHVA	RECOMENDACIÓN
	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			0	
	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 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 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		componente planificación			40	
PROMEDIO										**38**	**15,11111111**
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			60	
	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	53	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			40	
	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			40	
PROMEDIO										**48,1875**	**9,6375**
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			60	
	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			60	
	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			40	
PROMEDIO										**53,33333333**	**10,66666667**

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

COMPONENTE	ID	CARGO	ITEM	DESCRIPCIÓN	PRUEBA	CIBERSEGURIDAD	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO PHVA	RECOMENDACIÓN
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			40	
	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			60	0
PROMEDIO										50	10

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

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	40	40	CUMPLE	60	MENOR	60	MENOR	80	MENOR	100	MENOR
R2	n/a	Se clasifican los activos de información lógicos y físicos de la Ent	Administrativas	AD.4.2.1	40	20	MAYOR	40	CUMPLE	60	MENOR	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	40	20	MAYOR	40	CUMPLE	60	MENOR	80	MENOR	100	MENOR
			Administrativas	AD.1.1	40	20	MAYOR	40	CUMPLE	60	MENOR	80	MENOR	100	MENOR
			PHVA	P.4	40	20	MAYOR	40	CUMPLE	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	100	20	MAYOR	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
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	40	20	MAYOR	40	CUMPLE	60	MENOR	80	MENOR	100	MENOR
R7	n/a	Establecer y documentar el alcance, límites, política, procedimientos, roles y responsabilidades y del Modelo de Seguridad y Privacidad de la Información.	PHVA	P.1	40	60	MENOR	60	MENOR	60	MENOR	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	40	20	MAYOR	40	CUMPLE	60	MENOR	60	MENOR	80	MENOR
LIMITE DE MADUREZ INICIAL					480	260	MENOR	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

NIVEL	CUMPLE?
OPTIMIZADO	FALSO
GESTIONADO CUANTITATIVAMENTE	FALSO
DEFINIDO	FALSO
GESTIONADO	FALSO
INICIAL	FALSO

Nivel de madurez alcanzado	**NO ALCANZA NIVEL INICIAL**

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR															
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	40	N/A	N/A	60	MENOR	60	MENOR	80	MENOR	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	60	N/A	N/A	40	MAYOR	60	CUMPLE	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	45	N/A	N/A	40	MAYOR	60	MENOR	80	MENOR	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	40	N/A	N/A	40	CUMPLE	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	40	N/A	N/A	40	CUMPLE	60	MENOR	80	MENOR	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	100	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R18	n/a	Copias de seguridad	Tecnicas	T.4.3	100	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R19	n/a	Gestión de la vulnerabilidad técnica	Tecnicas	T.4.6	50	N/A	N/A	40	MAYOR	60	MENOR	80	MENOR	100	MENOR
E MADUREZ GESTIONADO					685	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	30	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R21	n/a	Seguridad ligada a los recursos humanos, durante la contratación	Administrativas	AD.3.2	47	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	60	N/A	N/A	N/A	N/A	60	CUMPLE	80	MENOR	100	MENOR
R23	n/a	Requisitos de negocio para el control de accesos.	Tecnicas	T.1.1	80	N/A	N/A	N/A	N/A	60	MAYOR	80	CUMPLE	100	MENOR
R24	n/a	Responsabilidades del usuario frente al control de accesos	Tecnicas	T.1.2.6	40	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR															
R25	n/a	Seguridad física y ambiental en áreas seguras	Tecnicas	T.1.3.1	100	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	100	CUMPLE
R26	n/a	Seguridad física y ambiental de los equipos	Tecnicas	T.3.2	73	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	85	N/A	N/A	N/A	N/A	60	MAYOR	80	MAYOR	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	55	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	30	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	47	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	60	N/A	N/A	N/A	N/A	60	CUMPLE	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	60	N/A	N/A	N/A	N/A	60	CUMPLE	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	0	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R36	n/a	Gestión de incidentes en la seguridad de la información, recopilación de evidencias.	Tecnicas	T.7.1.7	60	N/A	N/A	N/A	N/A	60	CUMPLE	80	MENOR	100	MENOR
R37	n/a	Implantación de la continuidad de la seguridad de la información.	Administrativas	AD.5.1.2	40	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	60	N/A	N/A	N/A	N/A	60	CUMPLE	80	MENOR	100	MENOR

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR

R39	Responsable de compras y adquisiciones	Gestión de la prestación del servicio por suministradores.	Administrativas	AD.7.2	40	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
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	0	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
DE MADUREZ DEFINIDO					452	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	PHVA	I.5	#N/D	N/A	N/A	N/A	N/A	N/A	N/A	80	#N/D	80	#N/D
			PHVA	E.1	60	N/A	N/A	N/A	N/A	N/A	N/A	40	MAYOR	60	CUMPLE
			PHVA	E.2	60	N/A	N/A	N/A	N/A	N/A	N/A	40	MAYOR	60	CUMPLE
			PHVA	E.3	40	N/A	N/A	N/A	N/A	N/A	N/A	40	CUMPLE	60	MENOR
			PHVA	M.1	40	N/A	N/A	N/A	N/A	N/A	N/A	40	CUMPLE	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 auditorias de acuerdo a lo establecido en el plan de auditorias 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	53	N/A	N/A	N/A	N/A	N/A	N/A	40	MAYOR	60	MENOR
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	60	N/A	N/A	N/A	N/A	N/A	N/A	60	CUMPLE	80	MENOR
R45	n/a	Registro de actividades en seguridad (bitácora operativa).	Tecnicas	T.4.4.1	40	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	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	60	N/A	N/A	N/A	N/A	N/A	N/A	60	CUMPLE	80	MENOR

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

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR															
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	60	N/A	N/A	N/A	N/A	N/A	N/A	60	CUMPLE	80	MENOR
R48	n/a	Gestión de acceso de usuario.	Tecnicas	T.1.2	50	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R49	n/a	Control de acceso a sistemas y aplicaciones	Tecnicas	T.1.4	72	N/A	N/A	N/A	N/A	N/A	N/A	60	MAYOR	80	MENOR
R50	n/a	Controles Criptográficos	Tecnicas	T.2.1	60	N/A	N/A	N/A	N/A	N/A	N/A	60	CUMPLE	80	MENOR
R51	n/a	Consideraciones de las auditorías de los sistemas de información	Tecnicas	T.4.4	45	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	60	N/A	N/A	N/A	N/A	N/A	N/A	60	CUMPLE	80	MENOR
R53	n/a	Cumplimiento de los requisitos legales y contractuales.	Administrativas	AD.6.1	40	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
Z GESTIONADO CUANTITATIVAMENTE					587	0		0		0		660	MENOR	880	MENOR
R55	n/a	Verificación, revisión y evaluación de la continuidad de la seguridad	Administrativas	AD.5.1.3	60	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	60	CUMPLE
LIMITE DE MADUREZ OPTIMIZADO					1134									1660	CUMPLE

FTIC-LP-09-15

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR							
FUNCIÓN NIST	**SUBCATEGORÍA NIST**	**CONTROL ANEXO A ISO 27001**	**CARGO**	**REQUISITO**	**HOJA**	**CALIFICACIÓN**	**FUNCIÓN 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	0	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	0	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	0	IDENTIFICAR
IDENTIFICAR	ID.GV-4	n/a	Responsable de SI	ón de riesgos tiene en cuenta los riesgos de ciberse	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	0	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	0	RECUPERAR
IDENTIFICAR	ID.RA-3	n/a	Responsable de SI	Las amenazas internas y externas son identificadas y documentadas.	n/a	0	IDENTIFICAR
RESPONDER	RS.IM-2	n/a	Responsable de SI	Las estrategias de respuesta se actualizan	n/a	0	RESPONDER

FTIC-LP-09-15

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR							
FUNCIÓN NIST	**SUBCATEGORÍA NIST**	**CONTROL ANEXO A ISO 27001**	**CARGO**	**REQUISITO**	**HOJA**	**CALIFICACIÓN**	**FUNCIÓN CSF**
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	0	IDENTIFICAR
IDENTIFICAR	ID.RA-4	n/a	Responsable de SI	Los impactos potenciales en la entidad y su probabilidad son identificados	n/a	0	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	0	RECUPERAR
PROTEGER	PR.IP-7	n/a	Responsable de SI	Los procesos de protección son continuamente mejorados	n/a	0	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	0	DETECTAR
IDENTIFICAR	ID.GV-1	A.5.1.1	n/a	n/a	Administrativas	40	IDENTIFICAR
IDENTIFICAR	ID.AM-6	A.6.1.1	n/a	n/a	Administrativas	40	IDENTIFICAR
IDENTIFICAR	ID.GV-2	A.6.1.1	n/a	n/a	Administrativas	40	IDENTIFICAR
PROTEGER	PR.AT-2	A.6.1.1	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.AT-3	A.6.1.1	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.AT-4	A.6.1.1	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.AT-5	A.6.1.1	n/a	n/a	Administrativas	40	PROTEGER
DETECTAR	DE.DP-1	A.6.1.1	n/a	n/a	Administrativas	40	DETECTAR
RESPONDER	RS.CO-1	A.6.1.1	n/a	n/a	Administrativas	40	RESPONDER
PROTEGER	PR.AC-4	A.6.1.2	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.DS-5	A.6.1.2	n/a	n/a	Administrativas	40	PROTEGER
RESPONDER	RS.CO-3	A.6.1.2	n/a	n/a	Administrativas	40	RESPONDER
RESPONDER	RS.CO-2	A.6.1.3	n/a	n/a	Administrativas	40	RESPONDER
IDENTIFICAR	ID.RA-2	A.6.1.4	n/a	n/a	Administrativas	40	IDENTIFICAR
PROTEGER	PR.IP-2	A.6.1.5	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.AC-3	A.6.2.2	n/a	n/a	Administrativas	80	PROTEGER
PROTEGER	PR.DS-5	A.7.1.1	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.IP-11	A.7.1.1	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.DS-5	A.7.1.2	n/a	n/a	Administrativas	20	PROTEGER
IDENTIFICAR	ID.GV-2	A.7.2.1	n/a	n/a	Administrativas	40	IDENTIFICAR

FTIC-LP-09-15

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR							
FUNCIÓN NIST	**SUBCATEGORÍA NIST**	**CONTROL ANEXO A ISO 27001**	**CARGO**	**REQUISITO**	**HOJA**	**CALIFICACIÓN**	**FUNCIÓN CSF**
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	60	PROTEGER
PROTEGER	PR.IP-11	A.7.3.1	n/a	n/a	Administrativas	60	PROTEGER
IDENTIFICAR	ID AM-1	A.8.1.1	n/a	n/a	Administrativas	40	IDENTIFICAR
IDENTIFICAR	ID AM-2	A.8.1.1	n/a	n/a	Administrativas	40	IDENTIFICAR
IDENTIFICAR	ID.AM-5	A.8.1.1	n/a	n/a	Administrativas	40	IDENTIFICAR
IDENTIFICAR	ID AM-1	A.8.1.2	n/a	n/a	Administrativas	40	IDENTIFICAR
IDENTIFICAR	ID AM-2	A.8.1.2	n/a	n/a	Administrativas	40	IDENTIFICAR
PROTEGER	PR.IP-11	A.8.1.4	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.DS-5	A.8.2.2	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.PT-2	A.8.2.2	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.DS-1	A.8.2.3	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.DS-2	A.8.2.3	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.DS-3	A.8.2.3	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.DS-5	A.8.2.3	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.IP-6	A.8.2.3	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.PT-2	A.8.2.3	n/a	n/a	Administrativas	60	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	0	PROTEGER
PROTEGER	PR.IP-6	A.8.3.2	n/a	n/a	Administrativas	0	PROTEGER
PROTEGER	PR.DS-3	A.8.3.3	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.PT-2	A.8.3.3	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.DS-5	A.9.1.1	n/a	n/a	Técnicas	100	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	40	PROTEGER
PROTEGER	PR.AC-4	A.9.2.3	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-5	A.9.2.3	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.AC-1	A.9.2.4	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.AC-1	A.9.3.1	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.AC-4	A.9.4.1	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.DS-5	A.9.4.1	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.AC-1	A.9.4.2	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.AC-1	A.9.4.3	n/a	n/a	Técnicas	20	PROTEGER
PROTEGER	PR.AC-4	A.9.4.4	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-5	A.9.4.4	n/a	n/a	Técnicas	40	PROTEGER
PROTEGER	PR.DS-5	A.9.4.5	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.AC-2	A.11.1.1	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.AC-2	A.11.1.2	n/a	n/a	Técnicas	40	PROTEGER

FTIC-LP-09-15

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR							
FUNCIÓN NIST	**SUBCATEGORÍA NIST**	**CONTROL ANEXO A ISO 27001**	**CARGO**	**REQUISITO**	**HOJA**	**CALIFICACIÓN**	**FUNCIÓN CSF**
PROTEGER	PR.MA-1	A.11.1.2	n/a	n/a	Técnicas	40	PROTEGER
IDENTIFICAR	ID.BE-5	A.11.1.4	n/a	n/a	Técnicas	100	IDENTIFICAR
PROTEGER	PR.AC-2	A.11.1.4	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.IP-5	A.11.1.4	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.AC-2	A.11.1.6	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.IP-5	A.11.2.1	n/a	n/a	Técnicas	40	PROTEGER
IDENTIFICAR	ID.BE-4	A.11.2.2	n/a	n/a	Técnicas	60	IDENTIFICAR
PROTEGER	PR.IP-5	A.11.2.2	n/a	n/a	Técnicas	60	PROTEGER
IDENTIFICAR	ID.BE-4	A.11.2.3	n/a	n/a	Técnicas	100	IDENTIFICAR
PROTEGER	PR.AC-2	A.11.2.3	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.IP-5	A.11.2.3	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.MA-1	A.11.2.4	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.MA-2	A.11.2.4	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.MA-1	A.11.2.5	n/a	n/a	Técnicas	60	PROTEGER
IDENTIFICAR	ID.AM-4	A.11.2.6	n/a	n/a	Técnicas	100	IDENTIFICAR
PROTEGER	PR.DS-3	A.11.2.7	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.IP-6	A.11.2.7	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.PT-2	A.11.2.9	n/a	n/a	Técnicas	0	PROTEGER
PROTEGER	PR.IP-1	A.12.1.2	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.IP-3	A.12.1.2	n/a	n/a	Técnicas	100	PROTEGER
IDENTIFICAR	ID.BE-4	A.12.1.3	n/a	n/a	Técnicas	100	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	100	PROTEGER
DETECTAR	DE.CM-4	A.12.2.1	n/a	n/a	Técnicas	100	DETECTAR
RESPONDER	RS.MI-2	A.12.2.1	n/a	n/a	Técnicas	100	RESPONDER
PROTEGER	PR.DS-4	A.12.3.1	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.IP-4	A.12.3.1	n/a	n/a	Técnicas	100	PROTEGER
PROTEGER	PR.PT-1	A.12.4.1	n/a	n/a	Técnicas	40	PROTEGER
DETECTAR	DE.CM-3	A.12.4.1	n/a	n/a	Técnicas	40	DETECTAR
RESPONDER	RS.AN-1	A.12.4.1	n/a	n/a	Técnicas	40	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	40	PROTEGER
RESPONDER	RS.AN-1	A.12.4.3	n/a	n/a	Técnicas	40	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	40	PROTEGER
PROTEGER	PR.IP-3	A.12.6.2	n/a	n/a	Técnicas	40	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

FTIC-LP-09-15

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR							
FUNCIÓN NIST	**SUBCATEGORÍA NIST**	**CONTROL ANEXO A ISO 27001**	**CARGO**	**REQUISITO**	**HOJA**	**CALIFICACIÓN**	**FUNCIÓN CSF**
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	60	IDENTIFICAR
PROTEGER	PR.AC-5	A.13.2.1	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.AC-3	A.13.2.1	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.DS-2	A.13.2.1	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.DS-5	A.13.2.1	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.PT-4	A.13.2.1	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.DS-2	A.13.2.3	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.DS-5	A.13.2.3	n/a	n/a	Técnicas	60	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	0	PROTEGER
PROTEGER	PR.DS-2	A.14.1.2	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.DS-5	A.14.1.2	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.DS-6	A.14.1.2	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.DS-2	A.14.1.3	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.DS-5	A.14.1.3	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.DS-6	A.14.1.3	n/a	n/a	Técnicas	60	PROTEGER
PROTEGER	PR.IP-2	A.14.2.1	n/a	n/a	Técnicas	60	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	60	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	40	DETECTAR
DETECTAR	DE.DP-3	A.14.2.8	n/a	n/a	Técnicas	60	DETECTAR
PROTEGER	PR.IP-9	A.16.1.1	n/a	n/a	Técnicas	0	PROTEGER
DETECTAR	DE.AE-2	A.16.1.1	n/a	n/a	Técnicas	0	DETECTAR
RESPONDER	RS.CO-1	A.16.1.1	n/a	n/a	Técnicas	0	RESPONDER
DETECTAR	DE.DP-4	A.16.1.2	n/a	n/a	Técnicas	60	DETECTAR
RESPONDER	RS.CO-2	A.16.1.3	n/a	n/a	Técnicas	0	RESPONDER
DETECTAR	DE.AE-2	A.16.1.4	n/a	n/a	Técnicas	40	DETECTAR
RESPONDER	RS.AN-4	A.16.1.4	n/a	n/a	Técnicas	40	RESPONDER
RESPONDER	RS.RP-1	A.16.1.5	n/a	n/a	Técnicas	60	RESPONDER
RESPONDER	RS.AN-1	A.16.1.5	n/a	n/a	Técnicas	60	RESPONDER
RESPONDER	RS.MI-2	A.16.1.5	n/a	n/a	Técnicas	60	RESPONDER
RECUPERAR	RC.RP-1	A.16.1.5	n/a	n/a	Técnicas	60	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	60	RESPONDER
IDENTIFICAR	ID.BE-5	A.17.1.1	n/a	n/a	Administrativas	40	IDENTIFICAR
PROTEGER	PR.IP-9	A.17.1.1	n/a	n/a	Administrativas	40	PROTEGER
IDENTIFICAR	ID.BE-5	A.17.1.2	n/a	n/a	Administrativas	40	IDENTIFICAR
PROTEGER	PR.IP-4	A.17.1.2	n/a	n/a	Administrativas	40	PROTEGER

FTIC-LP-09-15

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA

HOJA LEVANTAMIENTO DE INFORMACIÓN

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR-ICULTUR							
FUNCIÓN NIST	**SUBCATEGORÍA NIST**	**CONTROL ANEXO A ISO 27001**	**CARGO**	**REQUISITO**	**HOJA**	**CALIFICACIÓN**	**FUNCIÓN CSF**
PROTEGER	PR.IP-9	A.17.1.2	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.IP-9	A.17.1.2	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.IP-4	A.17.1.3	n/a	n/a	Administrativas	40	PROTEGER
PROTEGER	PR.IP-10	A.17.1.3	n/a	n/a	Administrativas	40	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	40	IDENTIFICAR
PROTEGER	PR.IP-4	A.18.1.3	n/a	n/a	Administrativas	0	PROTEGER
DETECTAR	DE.DP-2	A.18.1.4	n/a	n/a	Administrativas	40	DETECTAR
PROTEGER	PR.IP-12	A.18.2.2	n/a	n/a	Administrativas	60	PROTEGER
IDENTIFICAR	ID.RA-1	A.18.2.3	n/a	n/a	Administrativas	60	IDENTIFICAR
IDENTIFICAR	ID.BE-1	A.15.1	n/a	n/a	Administrativas	60	IDENTIFICAR
IDENTIFICAR	ID.BE-1	A.15.2	n/a	n/a	Administrativas	40	IDENTIFICAR
PROTEGER	PR.MA-2	A.15.1	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.MA-2	A.15.2	n/a	n/a	Administrativas	40	PROTEGER
DETECTAR	DE.CM-6	A.15.2	n/a	n/a	Administrativas	40	DETECTAR