DECLARACIÓN DE APLICABILIDAD CAS

ítem	Control	item-control	Aplica	Observaciones	Responsable de ejecucción	Tipo control
A.5.1.1	Políticas para la seguridad de la información	A.5.1.1Políticas para la seguridad de la información	Si	M-PGT-001-manual-de-politicas-de-seguridad-de-la-informacion v 4.0	GIT	
A.5.1.2	Revisión de las políticas para seguridad de la información	A.5.1.2Revisión de las políticas para seguridad de la información	Si	Definido según aprobación del comité de gestión institucional	GIT	
A.6.1.1	Roles y responsabilidades para la seguridad de información	A.6.1.1Roles y responsabilidades para la seguridad de información	Si	Delegados por comité instucional a la oficina de GIT CAS	GIT	
A.6.1.2	Separación de deberes	A.6.1.2Separación de deberes	Si	Definidos a través de los manuales de funciones institucionales y obligaciones en contrato de prestación de servicios.		
A.6.1.3	Contacto con las autoridades	A.6.1.3Contacto con las autoridades	Si	Se debe definir y actualizar la matriz de autoridades para casos relevantes de seguridad de la información.		
A.6.1.4	Contacto con grupos de interés especial	A.6.1.4Contacto con grupos de interés especial	Si	Se debe tener matrices adecuadas y grupos de interés a fin a la seguridad y privacidad de la información en el entorno público, como proveedores o sitios que publiquen contenido a fin.		
A.6.1.5	Seguridad de la información en la gestión de proyectos	A.6.1.5Seguridad de la información en la gestión de proyectos	Si	Se debe incluir en los proyectos a ejecutar evaluaciones de seguridad de la información de acuerdo con los temas o activos a tratar en la entidad.		
A.6.2.1	Política para dispositivos móviles	A.6.2.1Política para dispositivos móviles	Si	La política de dispositivos móviles se debe construir y socializar para evitar el uso indebido en los entornos corporativos.		
A.6.2.2	Teletrabajo	A.6.2.2Teletrabajo	Si	Se deben construir lineamiento de trabajo remoto y teletrabajo según las consideraciones de la legislación vigente en Colombia y circunstancias excepcionales por la emergencia sanitaria actual.		
A.7.1.1	Selección	A.7.1.1Selección	Si	Se deben alinear los procesos de selección acorde a las políticas de seguridad y privacidad de la entidad a demás de la legislación vigente en procesos de selección como las de la CNSC		
A.7.1.2	Términos y condiciones del empleo	A.7.1.2Términos y condiciones del empleo	Si	Se deben alinear los procesos de selección acorde a las políticas de seguridad y privacidad de la entidad además de la legislación vigente en procesos de selección como las de la CNSC		
A.7.2.1	Responsabilidades de la dirección	A.7.2.1Responsabilidades de la dirección	Si	Se debe consolidar el MSPI y el comité de gestión institucional de las políticas de gobierno Digital		
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	A.7.2.2Toma de conciencia, educación y formación en la seguridad de la información	Si	Se debe construir el plan de sensibilización y toma de conciencia de la seguridad digital, así como la socialización de acciones y políticas para fortalecer la cultura corporativa de seguridad digital.		
A.7.2.3	Proceso disciplinario	A.7.2.3Proceso disciplinario	Si	Se cumple mediante los procesos de las oficinas de control interno y disciplinario de la CAS.		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	A.7.3.1Terminación o cambio de responsabilidades de empleo	Si	Definidas en los procedimientos del área administrativa y de talento humano de la corporación.		
A.8.1.1	Inventario de activos	A.8.1.1Inventario de activos	Si	Se construirá el inventario de activos y socializará con cada área que aprobará su gestión y pertenencia de activos tanto tecnológicos como documentales.		
A.8.1.2	Propiedad de los activos	A.8.1.2Propiedad de los activos	Si	Definido ene l inventario de activos		
A.8.1.3	Uso aceptable de los activos	A.8.1.3Uso aceptable de los activos	Si	Se construirá y socializará las instrucciones para la gestión de activos a nivel de usuario final y las recomendaciones de su buen uso.		
A.8.1.4	Devolución de activos	A.8.1.4Devolución de activos	Si	Definido en los procedimientos de devolución de equipos.		
A.8.2.1	Clasificación de la información	A.8.2.1Clasificación de la información	Si	Se cumple de acuerdo con la ley 1712 2014		
A.8.2.2	Etiquetado de la información	A.8.2.2Etiquetado de la información	Si	Se cumple de acuerdo con la ley 1712 2014		
A.8.2.3	Manejo de activos	A.8.2.3Manejo de activos	Si	Se cumple de acuerdo con la ley 1712 2014		
A.8.3.1	Gestión de medios removibles	A.8.3.1Gestión de medios removibles	Si	Por definir el control		
A.8.3.2	Disposición de los medios	A.8.3.2Disposición de los medios	Si	Por definir el control		
A.8.3.3	Transferencia de medios físicos	A.8.3.3Transferencia de medios físicos	Si	Por definir el control		
A.9.1.1	Política de control de acceso	A.9.1.1Política de control de acceso	Si	Por definir el control		
A.9.1.2	Política sobre el uso de los servicios de red	A.9.1.2Política sobre el uso de los servicios de red	Si	Se construirá y socializará las instrucciones para la gestión de activos a nivel de usuario final y las recomendaciones de su buen uso.		
A.9.2.1	Registro y cancelación del registro de usuarios	A.9.2.1Registro y cancelación del registro de usuarios	Si	Por definir el control		
A.9.2.2	Suministro de acceso de usuarios	A.9.2.2Suministro de acceso de usuarios	Si	Por definir el control		
A.9.2.3	Gestión de derechos de acceso privilegiado	A.9.2.3Gestión de derechos de acceso privilegiado	Si	Por definir el control		
A.9.2.4	Gestión de información de autenticación secreta de usuarios	A.9.2.4Gestión de información de autenticación secreta de usuarios	Si	Por definir el control		
A.9.2.5	Revisión de los derechos de acceso de usuarios	A.9.2.5Revisión de los derechos de acceso de usuarios	Si	Por definir el control		
A.9.2.6	Retiro o ajuste de los derechos de acceso	A.9.2.6Retiro o ajuste de los derechos de acceso	Si	Por definir el control		
A.9.3.1	Uso de la información de autenticación secreta	A.9.3.1Uso de la información de autenticación secreta	Si	Por definir el control		
A.9.4.1	Restricción de acceso Información	A.9.4.1Restricción de acceso Información	Si	Por definir el control		
A.9.4.2	Procedimiento de ingreso seguro	A.9.4.2Procedimiento de ingreso seguro	Si	Por definir el control		
A.9.4.3	Sistema de gestión de contraseñas	A.9.4.3Sistema de gestión de contraseñas	Si	Por definir el control		
A.9.4.4	Uso de programas utilitarios privilegiados	A.9.4.4Uso de programas utilitarios privilegiados	Si	Por definir el control		
A.9.4.5	Control de acceso a códigos fuente de programas	A.9.4.5Control de acceso a códigos fuente de programas	No	No se tiene desarrollos interno o códigos fuentes almacenados.		
A.10.1.1	Política sobre el uso de los servicios de red	A.10.1.1Política sobre el uso de los servicios de red	Si	Por definir el control		
A.10.1.2	Gestión de llaves	A.10.1.2Gestión de llaves	Si	Por definir el control		
A.11.1.1	Perímetro de seguridad física	A.11.1.1Perímetro de seguridad física	Si	Sí contamos con un centro de datos y áreas de contabilidad con operaciones sensibles, pero No tenemos áreas de procesamiento de archivos confidenciales		
A.11.1.2	Controles físicos de entrada	A.11.1.2Controles físicos de entrada	Si	si tenemos tarjetas de acceso en el centro de Datos		
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	A.11.1.3Seguridad de oficinas, recintos e instalaciones	Si	Mediante contratos de vigilancia en las sedes de la CAS		
A.11.1.4	Protección contra amenazas externas y ambientales	A.11.1.4Protección contra amenazas externas y ambientales	Si	Se cuenta con controles de temperaturas en el centro de datos, extitores y medidas de precauciones para inundaciones		

A.11.1.5	Trabajo en áreas seguras	A.11.1.5Trabajo en áreas seguras	Si	Se tiene el Procedimiento para la Identificación de peligros y Riesgos		
A.11.1.6	Áreas de despacho y carga	A.11.1.6Áreas de despacho y carga	Si	El sótano del edificio principal tiene definida un área para carga y descarga con la vigilancia respectiva		
A.11.2.1	Ubicación y protección de los equipos	A.11.2.1Ubicación y protección de los equipos	Si	Los equipos de escritorio tienen los controles para evitar este tipo de accidentes así como se cuentan con pólizas que cubren los equipos informáticos, el centro de datos cumple también con las normas contra accidentes		
A.11.2.2	Servicios de suministro	A.11.2.2Servicios de suministro	Si	Por definir el control		
A.11.2.3	Seguridad del cableado	A.11.2.3Seguridad del cableado	Si	Por definir control		
A.11.2.4	Mantenimiento de equipos	A.11.2.4Mantenimiento de equipos	Si	Se realizan mantenimientos a equipos propios de la CAS		
A.11.2.5	Retiro de activos	A.11.2.5Retiro de activos	Si	Por definir el control		
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	A.11.2.6Seguridad de equipos y activos fuera de las instalaciones	Si	Por definir el control		
A.11.2.7	Disposición segura o reutilización de equipos	A.11.2.7Disposición segura o reutilización de equipos	Si	Por definir el control		
A.11.2.8	Equipos de usuario desatendidos	A.11.2.8Equipos de usuario desatendidos	Si	Por definir control		
A.11.2.9	Política de escritorio limpio y pantalla limpia	A.11.2.9Política de escritorio limpio y pantalla limpia	Si	Por definir control		
A.12.1.1	Procedimientos de operación documentados	A.12.1.1Procedimientos de operación documentados	Si	Se tiene procedimiento para el Mantenimiento Preventivo, Procedimiento para el Soporte al Hardware, Software, Redes y Aplicativos en General, Procedimiento para el Mantenimiento Correctivo, Procedimiento Control de Cambios del Software, Procedimiento para la Actualización de la Página Web		
A.12.1.2	Gestión de cambios	A.12.1.2Gestión de cambios	Si	Por definir control		
A.12.1.3	Gestión de capacidad	A.12.1.3Gestión de capacidad	Si	Por definir control		
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	A.12.1.4Separación de los ambientes de desarrollo, pruebas y operación	Si	Por definir el control		
A.12.2.1	Controles contra códigos maliciosos	A.12.2.1Controles contra códigos maliciosos	Si	Se cuenta con licencias de ESET NOD32 Antivirus suficiente		
A.12.3.1	Respaldo de información	A.12.3.1Respaldo de información	Si	Las copias de seguridad y la herramienta en Veeam backup, se realiza todos los días backup de los servidores en producción		
A.12.4.1	Registro de eventos	A.12.4.1Registro de eventos	Si	Por definir el control		
A.12.4.2	Protección de la información de registro	A.12.4.2Protección de la información de registro	Si	Por definir el control		
A.12.4.3	Registros del administrador y del operado	A.12.4.3Registros del administrador y del operado	Si	Por definir el control		
A.12.4.4	Sincronización de relojes	A.12.4.4Sincronización de relojes	Si	Por definir el control		
A.12.5.1	Instalación de software en sistemas operativos	A.12.5.1Instalación de software en sistemas operativos	Si	Por definir el control		
A.12.6.1	Gestión de las vulnerabilidades técnicas	A.12.6.1Gestión de las vulnerabilidades técnicas	Si	Por definir el control		
A.12.6.2	Restricciones sobre la instalación de software	A.12.6.2Restricciones sobre la instalación de software	Si	Por definir el control		
A.12.7.1	Información controles de auditoría de sistemas	A.12.7.1Información controles de auditoría de sistemas	Si	Por definir el control		
A.13.1.1	Controles de redes	A.13.1.1Controles de redes	Si	Por definir el control		
A.13.1.2	Seguridad de los servicios de red	A.13.1.2Seguridad de los servicios de red	Si	Por definir el control		
A.13.1.3	Separación en las redes	A.13.1.3Separación en las redes	Si	Por definir el control		
A.13.2.1	Políticas y procedimientos de transferencia de información	A.13.2.1Políticas y procedimientos de transferencia de información	Si	Por definir el control		
A.13.2.2	Acuerdos sobre transferencia de información	A.13.2.2Acuerdos sobre transferencia de información	Si	Por definir el control		
A.13.2.3	Mensajería electrónica	A.13.2.3Mensajería electrónica	Si	Se asignan correos electrónicos mediante solicitud firmada por jefe de oficina y el solicitante, Si se usan certificados SSL y el proveedor de hosting protege mediante firewall el envío y recepción de correos		
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	A.13.2.4Acuerdos de confidencialidad o de no divulgación	Si	Se cuenta con el Acuerdo de Confidencialidad para todos los funcionarios y contratistas		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	A.14.1.1Análisis y especificación de requisitos de seguridad de la información	Si	Por definir el control		
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	A.14.1.2Seguridad de servicios de las aplicaciones en redes publicas	Si	Por definir el control		
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	A.14.1.3Protección de transacciones de los servicios de las aplicaciones	Si	Por definir el control		
A.14.2.1	Política de desarrollo seguro	A.14.2.1Política de desarrollo seguro	No	No se tiene desarrollos interno o códigos fuentes almacenados.		
A.14.2.2	Procedimientos de control de cambios en sistemas	A.14.2.2Procedimientos de control de cambios en sistemas	No	No se tiene desarrollos interno o códigos fuentes almacenados.		
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	A.14.2.3Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	No	No se tiene desarrollos interno o códigos fuentes almacenados.		
A.14.2.4	Restricciones en los cambios a los paquetes de software	A.14.2.4Restricciones en los cambios a los paquetes de software	No	No se tiene desarrollos interno o códigos fuentes almacenados.		
A.14.2.5	Principios de construcción de sistemas seguros	A.14.2.5Principios de construcción de sistemas seguros	No	No se tiene desarrollos interno o códigos fuentes almacenados.		
A.14.2.6	Ambiente de desarrollo seguro	A.14.2.6Ambiente de desarrollo seguro	No	No se tiene desarrollos interno o códigos fuentes almacenados.		
A.14.2.7	Desarrollo contratado externamente	A.14.2.7Desarrollo contratado externamente	Si	Por definir el control		
A.14.2.8	Pruebas de seguridad de sistemas	A.14.2.8Pruebas de seguridad de sistemas	No	No se tiene desarrollos interno o códigos fuentes almacenados.		
A.14.2.9	Prueba de aceptación de sistemas	A.14.2.9Prueba de aceptación de sistemas	Si	Por definir el control		
A.14.3.1	Protección de datos de prueba	A.14.3.1Protección de datos de prueba	No	No se tiene desarrollos interno o códigos fuentes almacenados.		
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	A.15.1.1Política de seguridad de la información para las relaciones con proveedores	Si	Por definir el control		
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	A.15.1.2Tratamiento de la seguridad dentro de los acuerdos con proveedores	Si	Por definir el control		
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	A.15.1.3Cadena de suministro de tecnología de información y comunicación	Si	Por definir el control		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	A.15.2.1Seguimiento y revisión de los servicios de los proveedores	Si	Por definir el control		
A.15.2.2	Gestión de cambios en los servicios de proveedores	A.15.2.2Gestión de cambios en los servicios de proveedores	Si	Por definir el control		

A.16.1.1	Responsabilidad y procedimientos de gestión de incidentes	A.16.1.1Responsabilidad y procedimientos de gestión de incidentes	Si	Por definir el control		
A.16.1.2	Reporte de eventos de seguridad de la información	A.16.1.2Reporte de eventos de seguridad de la información	Si	Por definir el control		
A.16.1.3	Reporte de debilidades de seguridad de la información	A.16.1.3Reporte de debilidades de seguridad de la información	Si	Por definir el control		
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	A.16.1.4Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Si	Por definir el control		
A.16.1.5	Respuesta a incidentes de seguridad de la información	A.16.1.5Respuesta a incidentes de seguridad de la información	Si	Por definir el control		
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	A.16.1.6Aprendizaje obtenido de los incidentes de seguridad de la información	Si	Por definir el control		
A.16.1.7	Recolección de evidencia	A.16.1.7Recolección de evidencia	Si	Por definir el control		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	A.17.1.1Planificación de la continuidad de la seguridad de la información	Si	Por definir el control		
A.17.1.2	Implementación de la continuidad de la seguridad de la información	A.17.1.2Implementación de la continuidad de la seguridad de la información	Si	Por definir el control		
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	A.17.1.3Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Si	Por definir el control		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	A.17.2.1Disponibilidad de instalaciones de procesamiento de información	Si	Por definir el control		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	A.18.1.1Identificación de la legislación aplicable y de los requisitos contractuales	Si	El área jurídica evaluara los riesgos legales y matrices de cumplimiento a demás de evaluar y aportar el respectivo normograma institucional para su funcionamiento acorde la legislación vigente.		
A.18.1.2	Derechos de propiedad intelectual	A.18.1.2Derechos de propiedad intelectual	Si	Los contratos incluyen cláusulas de protección al trabajo realizado y propiedad intelectual		
A.18.1.3	Protección de registros	A.18.1.3Protección de registros	Si			
A.18.1.4	Privacidad y protección de datos personales	A.18.1.4Privacidad y protección de datos personales	Si	Actualmente se tiene la política de protección de datos personales publicada y socializada en sitios web e Intranet de la CAS		
A.18.1.5	Reglamentación de controles criptográficos	A.18.1.5Reglamentación de controles criptográficos	Si	Se evaluará los controles y reglamentos pertinentes de acuerdo con los sistemas, proyecto u otras iniciativas que requiera proteger la información con algoritmos criptográficos.		
A.18.2.1	Revisión independiente de la seguridad de la información	A.18.2.1Revisión independiente de la seguridad de la información	Si	Por definir procesos de revisión externa de seguridad.		
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	A.18.2.2Cumplimiento con las políticas y normas de seguridad	Si	Se realizarán seguimientos internos y por entidades gubernamentales de control el avance de la política de seguridad digital.		
A.18.2.3	Revisión del cumplimiento técnico	A.18.2.3Revisión del cumplimiento técnico	Si	El área TIC evaluara regularmente los controles existentes con el fin de endurecer e identificar adecuadamente los controles pertinentes para la seguridad Digital.		