MINISTERIO DEL DEPORTE

DECLARACIÓN DE APLICABILIDAD

VERSIÓN 4
AGOSTO DE 2022

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	APLICA SI	APLICA NO	JUSTIFICACIÓN
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**				
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	X		Se cuenta con la Política General de Seguridad de la Información, la cual fue aprobada por el Comité Institucional de Gestión y Desempeño para la actual vigencia.
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		X		Se realiza al menos una revisión anual que permite asegurar su conveniencia, adecuación y eficacia continua.
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**					
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**				
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	X		Las responsabilidades de la seguridad de la información están contenidas en la Política General de Seguridad de la Información
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	X		La resolución 02359 del 3 de diciembre de 2019 establece los grupos internos de trabajo del Ministerio del Deporte y asigna sus funciones
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	X		Se actualizó el documento GT-PD-007 PROCEDIMIENTO REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN y se anexó una matriz para el reporte de Actividades Informativas, Eventos e Incidentes de Seguridad de la Información.
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	X		Se mantiene el contacto con MinTIC, CSIRT, COLCERT para las actividades de formación en seguridad de la información
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	X		Se cuenta con el GT-PD-017 PROCEDIMIENTO PROYECTOS ESPECIALES DE TECNOLOGÍA
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**				
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			X		Dentro de la Política General de Seguridad de la Información de la entidad se cuenta con las secciones 4.3.6 DISPOSITIVOS MÓVILES, TRABAJO REMOTO EN CASA Y TELETRABAJO y 4.3.6.1. DIRECTRICES DISPOSITIVOS MÓVILES
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	X		Dentro de la Política General de Seguridad de la Información de la entidad se cuenta con las secciones 4.3.6. DISPOSITIVOS MÓVILES, TRABAJO REMOTO EN CASA Y TELETRABAJO y 4.3.6.3. DIRECTRICES TELETRABAJO
SEGURIDAD DE LOS RECURSOS HUMANOS									
AD.3	**Responsable de SI/Gestión Humana/Líderes de los procesos**	**SEGURIDAD DE LOS RECURSOS HUMANOS**		**A.7**					
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**				
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	X		La Politica General de Seguridad de la Información es de obligatorio cumplimiento por parte de funcionarios, contratistas y terceros que ejerzan funciones al interior de la entidad
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	X		Se realizan actividades regulares de formación en seguridad de la información
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**				
GESTIÓN DE ACTIVOS									
AD.4	**Responsable de SI**	**GESTIÓN DE ACTIVOS**		**A.8**					
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**				
AD.4.1.1	Responsable de SI	Inventario de activos	Se deben identificar los activos de información 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	X		Se cuenta con un inventario de activos actualizado y una actualización general anual.
AD.4.1.2	Responsable de SI	Propiedad de los activos	Los activos de información mantenidos en el inventario deben tener un propietario.	A.8.1.2		ID AM-1 ID AM-2	X		El inventario de activos de información relaciona el proceso al cual pertenecen
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			X		Se documentan en la Política General de Seguridad de la Información
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**					
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		X		En el inventario de activos de información se realiza la clasificación de acuerdo a los requisitos legales y la norma ISO 27001
AD.4.2.2	Responsable de SI	Etiquetado de la información		A.8.2.2		PR.DS-5 PR.PT-2	X		Se cuenta con el instructivo GD-IN-002 Organización Documental y Ubicación Topográfica

AD.4.2.3	Responsable de SI	Manejo de activos de información		A.8.2.3		PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-5 PR.IP-6 PR.PT-2	X	Se cuenta con el documento GT-PD-020 PROCEDIMIENTO GESTIÓN DEL INVENTARIO DE ACTIVOS DE INFORMACIÓN
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**				
AD.4.3.1	Responsable de TICs	Gestión de medios removibles		A.8.3.1		PR.DS-3 PR.IP-6 PR.PT-2	X	Se cuenta con la Política General de Seguridad de la Información, en la sección 4.2.EQUIPOS DE CÓMPUTO
AD.4.3.2	Responsable de TICs	Disposición de los medios		A.8.3.2		PR.DS-3 PR.IP-6	X	Se cuenta con la Política General de Seguridad de la Información, en la sección 4.2.8.ELIMINACIÓN SEGURA DE LA INFORMACIÓN DE EQUIPOS Y MEDIOS
AD.4.3.3	Responsable de TICs	Transferencia de medios físicos		A.8.3.3		PR.DS-3 PR.PT-2	X	Se cuenta con la Política General de Seguridad de la Información, en la sección 4.2.EQUIPOS DE CÓMPUTO
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO								
AD.5	**Responsables de toda la entidad en la Continuidad del negocio**	**SEGURIDAD DE LA INFORMACIÓN COMO COMPONENETE DE LA CONTINUIDAD DEL NEGOCIO**		**A.17**				
AD.5.1	**Responsables de toda la entidad en la Continuidad del negocio**	**Continuidad del negocio**	**SEGURIDAD DE LA INFORMACIÓN COMO COMPONENTE DE LA CONTINUIDAD DEL NEGOCIO**	**A.17.1**				
AD.5.1.1	Responsables de toda la entidad en la Continuidad del negocio	Planificación de la continuidad del negocio		A.17.1.1	Documentar controles para garantizar la continuidad del negocio	ID.BE-5 PR.IP-9	X	Se cuenta con el PLAN DE CONTINUIDAD DEL NEGOCIO
CUMPLIMIENTO								
AD.6	**Responsable de SI/Responsable de TICs/Control Interno**	**CUMPLIMIENTO**		**A.18**				
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**	**Modelo de Madurez Gestionado Cuantitativamente**	**ID.GV-3**		
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	X	Se cuenta con la Política de Protección de Datos Personales
AD.6.1.5	n/a	Reglamentación de controles criptográficos.		A.18.1.5			X	Dentro de la Política General de Seguridad de la entidad se cuenta con las secciones 4.3.9. USO DE CONTROLES CRIPTOGRÁFICOS PARA LA PROTECCIÓN DE LA INFORMACIÓN, 4.3.9.1. CONTROLES CRIPTOGRÁFICOS y 4.3.9.2. GENERACIÓN DE LLAVES CRIPTOGRÁFICAS EN EQUIPOS DE CÓMPUTO QUE ALMACENAN INFORMACIÓN CLASIFICADA Y RESERVADA
AD.6.2	**Control interno**	**Revisiones de seguridad de la información**		**A.18.2**	**Modelo de Madurez Gestionado Cuantitativamente**			
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	X	Se realizan actividades de hacking ético periódicamente
RELACIONES CON LOS PROVEEDORES								
AD.7	**Responsable de compras y adquisiciones**	**RELACIONES CON LOS PROVEEDORES**		**A.15**				
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		X	BS-MN-001 Manual de Contratación, Supervisión e Interventoría y anexos (Estudios previos), BS-PD-002 Supervisión, Interventoría y Seguimiento a la Ejecución Contractual
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		X	BS-MN-001 Manual de Contratación, Supervisión e Interventoría y anexos (Estudios previos), BS-PD-002 Supervisión, Interventoría y Seguimiento a la Ejecución Contractual
CONTROL DE ACCESO								
T.1	**Responsable de SI/Responsable de TICs**	**CONTROL DE ACCESO**		**A.9**	**Componente planificación y modelo de madurez nivel gestionado**			
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			
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.3.CONTROL DE ACCESO
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.6.INTERNET
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			
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.3.CONTROL DE ACCESO
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.3.CONTROL DE ACCESO
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.3.CONTROL DE ACCESO
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	X	Se cuenta con el documento GT-PD-013 PROCEDIMIENTO ADMINISTRACIÓN DE AUTENTICACIÓN Y PERMISOS
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			X	Se cuenta con el documento GT-PD-013 PROCEDIMIENTO ADMINISTRACIÓN DE AUTENTICACIÓN Y PERMISOS
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			X	Se cuentan con los controles para el retiro de los accesos una vez se termina la relación contractual
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			
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.10.LINEAMIENTOS GENERALES
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			

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	X		Se cuenta con la Política General de Seguridad de la Información, sección 4.3.CONTROL DE ACCESO
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	X		Sistema de Autenticación de Usuarios Directorio Activo, integración de los Sistemas de Información con el Directorio Activo. GT-PD-009 Administración de Autenticación y Permisos
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		X	Falta un sistema de gestión de contraseñas interactivo
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	X		Se cuenta con la Política General de Seguridad de la Información
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	X		Se cuenta con un proceso no escrito de restricción de acceso al código fuente
			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**					
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				
T.2.1.1	Responsable de SI	Política sobre el uso de controles criptográficos	Se deben desarrollar controles criptográficos para la protección de la información.	A.10.1.1			X		Dentro de la Política General de Seguridad de la entidad se cuenta con las secciones 4.3.9. USO DE CONTROLES CRIPTOGRÁFICOS PARA LA PROTECCIÓN DE LA INFORMACIÓN, 4.3.9.1. CONTROLES CRIPTOGRÁFICOS y 4.3.9.2. GENERACIÓN DE LLAVES CRIPTOGRÁFICAS EN EQUIPOS DE CÓMPUTO QUE ALMACENAN INFORMACIÓN CLASIFICADA Y RESERVADA
T.2.1.2	Responsable de SI	Gestión de llaves	Se deben desarrollar controles sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	A.10.1.2			X		Dentro de la Política General de Seguridad de la entidad se cuenta con las secciones 4.3.9. USO DE CONTROLES CRIPTOGRÁFICOS PARA LA PROTECCIÓN DE LA INFORMACIÓN, 4.3.9.1. CONTROLES CRIPTOGRÁFICOS y 4.3.9.2. GENERACIÓN DE LLAVES CRIPTOGRÁFICAS EN EQUIPOS DE CÓMPUTO QUE ALMACENAN INFORMACIÓN CLASIFICADA Y RESERVADA
			SEGURIDAD PERIMETRAL Y DE EQUIPOS						
T.3	**Responsable de SI**	**SEGURIDAD PERIMETRAL Y DE EQUIPOS**		**A.11**					
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				
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	X		Guaya de seguridad en equipos portátiles y precinto. Empresa de Vigilancia, Sistema de Control de Acceso y Cámaras de Seguridad. Sensores de Humo, sistema de Extinción de Incendio y Aire Acondicionado.
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	X		UPS Centro de cómputo. Red Regulada.
T.3.2.3	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	X		Plan de Mantenimiento Preventivo y Correctivo. Renovación Tecnológica.
T.3.2.4	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	X		Procedimiento para la autorización para retiro de equipos de la entidad
T.3.2.5	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	X		Polizas de Equipos de Computo. Autenticación con usuario y clave directorio activo.
T.3.2.6	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	X		Se cuenta con la Política General de Seguridad de la Información, sección 4.2.EQUIPOS DE CÓMPUTO
T.3.2.7	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			X		Se cuenta con la Política General de Seguridad de la Información, sección 4.2.EQUIPOS DE CÓMPUTO
			SEGURIDAD DE LAS OPERACIONES						
T.4	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS OPERACIONES**		**A.12**					
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				
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			X		Los procedimientos se encuentran documentados y dispuestos en la plataforma Isolución
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. Reunión periódica del Grupo Asesor de control de Cambios en Hardware y Software.	A.12.1.2		PR.IP-1 PR.IP-3	X		Los controles de seguridad de la información están contenidos en la matrices de riesgos por proceso disponibles en Isolución
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	X		Plan de Acción de Grupo Interno de Trabajo TIC´s y Plan Estratégico de Tecnologías de la Información PETI
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	X		Se cuenta con la Política General de Seguridad de la Información, sección 4.4.9.SEGURIDAD EN ENTORNOS DE DESARROLLO Y PRUEBA
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**					
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	X		Consola antivirus y protección de servidores, firewall SOPHOS y McAfee Endpoint Security
T.4.3	**Responsable de TICs**	**COPIAS DE RESPALDO**	**Proteger contra la pérdida de datos.**	**A.12.3**	Modelo de madurez gestionado				
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	X		GT-IN-001 Backup o Copias de Respaldo GT-MN-006Manual de Operación de la Política de Backups y Restauración de Información
T.4.4	Responsable de SI	**REGISTRO Y SEGUIMIENTO**	**Registrar eventos y generar evidencia.**	**A.12.4**	Modelo de madurez gestionado cuantitativamente				
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	X		Para servidores, esta habilitado en visor de eventos, registro de windows. Para la plaraforma Microsoft 365 esta habilitado el resgistro de eventos.
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	X		Registros de monitoreo protegidos Usuarios Administradores del Directorio Activo, GT-MN-002 Politicas de Seguridad de la Información:POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS

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	X	GT-MN-005 Manual de la Políticas de Seguridad Digital: POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS
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	X	GT-MN-005 Manual de la Políticas de Seguridad Digital : SINCRONIZACIÓN DE RELOJES
T.4.5	**Responsable de TICs**	**CONTROL DE SOFTWARE OPERACIONAL**	**Asegurar la integridad de los sistemas operacionales.**	**A.12.5**	Modelo de madurez definido			
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.6.2.USO PERMITIDO
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			
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	X	Análisis de vulnerabilidades periódicos
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.6.2.USO PERMITIDO
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			
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			X	No se han realizado actividades de auditoria
SEGURIDAD DE LAS COMUNICACIONES								
T.5	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS COMUNICACIONES**		**A.13**				
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			
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	X	Administración firewall SOPHOS y McAfee Endpoint Security
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			X	Se cuenta con el documento Plan de continuidad de los servicios tecnológicos acorde a los servicios de conectividad contratados
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	X	Red fragmentada Sede Adminsitrativa, CAR y WiFi.
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			
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	X	Falta documentar el procedimiento formal de transferencia de información
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			X	Falta documentar el procedimiento formal de transferencia de información
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	X	La plataforma Microsoft 365 cuenta con las certificaciones de seguridad que garantizan un nivel adecuado de protección de la mensajería
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	X	Cláusulas en los acuerdos contractuales
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS								
T.6	**Responsable de SI/Responsable de TICs**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		**A.14**				
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			
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.4.1.ADQUISICIÓN DE SOFTWARE O CONTRATACIÓN DE NUEVOS DESARROLLOS
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	X	Red fragmentada sede administrativa, CAR y WiFi.
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	X	Se cuenta con procedimientos no escritos para disponer de los servicios vía https
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			
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.4.SOFTWARE
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.4.SOFTWARE
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.4.SOFTWARE
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.4.SOFTWARE
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	X	Se cuenta con la Política General de Seguridad de la Información, sección 4.4.11. CONSTRUCCIÓN DE SISTEMAS SEGUROS
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			X	Se cuenta con la Política General de Seguridad de la Información, sección 4.4.SOFTWARE

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	X		BS-MN-001 Manual de Contratación, Supervisión e Interventoría, BS-PD-002 Supervisión, Interventoría y Seguimiento a la Ejecución Contractual.
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		X	Se realizan pruebas de vulnerabilidad pero falta un proceso formal de pruebas de seguridad
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			X		Se cuenta con la Política General de Seguridad de la Información, sección 4.4.3.DESARROLLO, CAMBIOS Y/O ACTUALIZACIONES DE SOFTWARE Y SISTEMAS
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				
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			X		Se cuenta con la Política General de Seguridad de la Información, sección 4.4.9.SEGURIDAD EN ENTORNOS DE DESARROLLO Y PRUEBA
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**					
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**					
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	X		Se cuenta con el documento S-105 GT-PD-007 PROCEDIMIENTO REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN y se cuenta con una Botácora de Incidentes
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	X		Se cuenta con el documento GT-PD-007 PROCEDIMIENTO REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
T.7.1.3	Responsable de SI	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	A.16.1.3	Modelo de madurez definido	RS.CO-2	X		Se cuenta con la Política General de Seguridad de la Información, sección 4.10.LINEAMIENTOS GENERALES
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	X		Se cuenta con el documento S-105 GT-PD-007 PROCEDIMIENTO REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN y se cuenta con una Botácora de Incidentes
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	X		Se cuenta con el documento S-105 GT-PD-007 PROCEDIMIENTO REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN y se cuenta con una Botácora de Incidentes
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		X	No hay un proceso de gestión de conocimiento
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	X		Se cuenta con el documento S-107 GT-PD-010 PROCEDIMIENTO RECOLECCIÓN DE EVIDENCIA DIGITAL