AUDITORÍA
GENERAL DE LA REPÚBLICA - COLOMBIA

Políticas de Seguridad de la información

OFICINA DE PLANEACIÓN

Bogotá, agosto de 2022

Contenido

Política seguridad de la información

La dirección de la AUDITORÍA GENERAL DE LA REPÚBLICA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un modelo de seguridad y privacidad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para La AUDITORÍA GENERAL DE LA REPÚBLICA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se define en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del MSPI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices y practicantes.
- Garantizar la continuidad del negocio frente a incidentes.

La AUDITORÍA GENERAL DE LA REPÚBLICA ha decidido definir, implementar, operar y mejorar de forma continua un modelo de Seguridad y privacidad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

1. Políticas técnicas de seguridad de la información:

1.1. Política uso de dispositivos móviles y teletrabajo.

1.1.1 Objetivo:

Definir las Lineamientos, responsables y soportes de las políticas de seguridad de la información: DISPOSITIVOS MÓVILES y TELETRABAJO con el fin de preservar la disponibilidad, integridad y confidencialidad de la información.

1.1.2 Alcance:

Lo definido en la presente guía aplica para los funcionarios y contratistas de la Auditoría General de La República.

1.1.3 Lineamientos de la política en dispositivos móviles.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	Llevar un registro y control de todos los dispositivos móviles (portátiles, tabletas y teléfonos móviles) que posee la AGR. (Entrega y recibido de los dispositivos) y hacer firmar por parte de los funcionarios y contratistas el compromiso de cumplimiento de controles.	Recursos Físicos	Inventario de dispositivos móviles Compromiso firmado cumplimiento de controles
	Definir un procedimiento formal de salida de dispositivos de las instalaciones, donde se especifique, entre otras cosas, que el uso de los equipos portátiles de propiedad de la AGR, fuera de las instalaciones, únicamente se permitirá a usuarios autorizados mediante una orden de salida, la cual debe tener el visto		Procedimiento de salida de dispositivos

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	bueno del jefe inmediato con firma autorizada para este fin		
	No permitir la salida de equipos de escritorio para la ejecución de cualquier actividad fuera de las instalaciones de la AGR. Cuando por alguna excepción se requiera la salida de un equipo de escritorio deberá tener la autorización previa del jefe directo y el grupo TIC, con el fin de verificar que tipo de información se encuentra almacenada en este y aplicar controles necesarios antes de su salida.		
	Hacer buen uso de los dispositivos móviles (portátiles, tabletas y teléfonos móviles) que son asignados para el desempeño de sus funciones laborales u obligaciones contractuales.	Funcionarios y contratistas de la AGR	Compromiso firmado de cumplimiento de controles para equipos móviles.
	Contar con un sistema de autenticación, como un patrón, código de desbloqueo o una clave, para todos los dispositivos móviles, como celulares, que almacenen información de la AGR		N/A
	Utilizar en los dispositivos móviles únicamente redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Utilizar los equipos móviles asignados por la AGR exclusivamente para desempeñar las funciones asignadas al cargo o las obligaciones contractuales pactadas.		
	El uso de los escritorios móviles asignados debe ser exclusivo del servidor público o contratista, por lo tanto, no debe realizar préstamos de estos.		
	Es responsabilidad del funcionario o contratista realizar periódicamente copias de respaldo a la información que se almacena en el dispositivo. En caso que el funcionario no sepa realizar un respaldo o una copia de seguridad se les brinda capacitación por parte del grupo TIC		
	No instalar ni configurar en los servicios ni en la infraestructura tecnológica de la AGR (computadores de escritorio, equipos móviles, servidores de cómputo físicos y virtuales, etc.) software para conexiones remotas gratis o de pago como *Teamviewer*, *AnyDesk* y otros, para realizar sesiones de trabajo extensas. Se debe utilizar VPN para las conexiones remotas.		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Implementación de los controles apropiados para proteger los dispositivos móviles, que son autorizados para salir de las instalaciones, como son: • Identificación de tipo de dispositivo. • Versión de aplicaciones instaladas. • Restricción en la ejecución de aplicaciones de acuerdo con las que están permitidas. • Contenido restringido, de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN, y de ser necesario, se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos entre otros.	Grupo TIC	Configuración de cada equipo, en los dispositivos de seguridad
	Asegurar que los dispositivos móviles provistos por la AGR cuenten con los siguientes controles: 1. Uso de usuario y contraseña para acceso al mismo. 2. Uso de software antivirus provisto por la AGR. 3. Restricción de privilegios administrativos para los usuarios.		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	4. Uso de software licenciado y provisto por la AGR (Software base) 5. Realización de copias de seguridad periódicas. 6. Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos como Drive o almacenamiento en la nube. 7. Adquisición de pólizas que cubran el hardware y la información de los dispositivos, contra pérdida o hurto.		

1.1.4 Lineamientos Teletrabajo.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Acatar el procedimiento de Teletrabajo establecido en la normatividad correspondiente vigente tanto externa como interna.	Funcionarios AGR	Compromiso firmado de cumplimiento de controles de seguridad de la información.
	Contar con un sistema de autenticación, como un código de desbloqueo o una clave, token o autenticación de doble factor, para el equipo de cómputo donde se utilizará el escritorio virtual, que almacene información de la AGR		

	Realizar periódicamente copias de respaldo de la información. Para la información almacenada en los escritorios virtuales que son entregados por la AGR.		
	El uso de los escritorios móviles asignados debe ser exclusivo del servidor público, por lo tanto, no debe realizar préstamos de estos; y solo se deben utilizar para asuntos laborales		
	Hacer cumplir el procedimiento de Teletrabajo establecido en la normatividad correspondiente vigente tanto externa como interna.	Talento Humano	
	Garantizar la aplicación de la política de dispositivos móviles	Grupo TIC	Configuración de cada equipo, en los dispositivos de seguridad

1.1.5 Lineamientos Trabajo remoto

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.	Contar con las aprobaciones requeridas para establecer conexión remota (VPN) a los dispositivos de la plataforma tecnológica de la AGR y acatar las instrucciones de acceso establecidas para las conexiones remotas.	Funcionarios y Contratistas AGR	Manual de acceso a VPN
	Establecer conexiones remotas únicamente a través de las VPN seguras y utilizar computadores en sitios confiables (Ej. Casa) y, en ninguna circunstancia, en		Manual de acceso a VPN

	computadores públicos, de hoteles o cafés internet, entre otros.		
	Realizar la solicitud de conexiones VPN por medio de la Mesa de Ayuda de Tecnología		CAU (centro de atención al usuario)
	El funcionario o contratista que solicite acceso por medio de una VPN es responsable del uso adecuado del acceso remoto.		CAU (centro de atención al usuario)
	Evaluar las solicitudes de permisos de VPN, aprobarlas o denegarlas.	Grupo TIC	CAU (centro de atención al usuario)
	Configurar las conexiones remotas a los servicios tecnológicos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores asignadas dentro de la AGR		CAU (centro de atención al usuario)

1.2 Política de seguridad de los recursos humanos

1.2.1 Objetivo:

Definir las Lineamientos, responsables y soportes de la política de seguridad de la información: SEGURIDAD DE LA INFORMACIÓN EN LOS RECURSOS HUMANOS, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información de la Auditoría General de la República – AGR.

1.2.2 Alcance:

Lo definido en la presente guía aplica para los funcionarios y contratistas de la AGR.

1.2.3 Lineamientos seguridad de los recursos humanos.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Se deben definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización	Definir y actualizar cuando se requiera los roles y responsabilidades de los servidores públicos y contratistas frente al MSPI - Políticas de seguridad	Grupo TIC	Matriz de roles y responsabilidades
	Definir en los procedimientos de la Entidad de acuerdo con la normatividad vigente, los mecanismos de verificación necesarios cuando las personas se postulan a los empleos durante la fase de selección del talento humano de planta y para la revisión de los antecedentes del personal a contratar.	Dirección Talento Humano / Oficina Jurídica	Procedimientos asociados a la selección y vinculación en el proceso de Gestión del Talento Humano y del Proceso de Contratación
	Definir los mecanismos de autorización para el tratamiento de los datos personales de los servidores públicos y contratistas de acuerdo con la Política de tratamiento de datos personales y de acuerdo con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios. Nota: La autorización para el tratamiento de datos personales asociados a		Procedimientos asociados a la selección y vinculación en el proceso de Gestión del Talento Humano / Formato autorización para el tratamiento de los datos personales de los contratistas en la fase de estudios previos de contratación directa.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	contratistas vinculados por modalidades diferentes a Contratación Directa se realiza a través de SECOP y a través del uso del módulo para cargue de información personal y/o confidencial de SECOP.		
	Enviar novedades de planta de servidores públicos o nuevos contratos al grupo TIC y a TH a través del mecanismo definido, con el fin que se realice una adecuada gestión de acceso físico por parte de TH y del acceso a los servicios TIC (gestión de usuarios) por parte del grupo TIC.	Dirección Talento Humano / Grupo TIC.	CAU (Centro de atención al usuario)
	Establecer los mecanismos del acuerdo de confidencialidad y no divulgación de la información y el compromiso de cumplimiento de los roles y responsabilidades frente a las políticas y lineamientos de seguridad y privacidad de la información, dicho documento debe reposar en la historia laboral o expediente contractual según sea el caso.	Dirección Talento Humano / Oficina Jurídica	Para funcionarios: Formato compromiso de confidencialidad Para contratistas: Anexo Clausulado General Contrato – Cláusula de confidencialidad. Pliegos de Condiciones

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Dar a conocer a los servidores públicos y contratistas nuevos, las políticas, roles, responsabilidades y obligaciones en materia de la seguridad de la información.	Dirección Talento Humano / Grupo TIC.	Proceso de Inducción y Reinducción Mecanismo de socialización para contratistas.
Asegurarse de que los servidores públicos y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	Tomar las acciones pertinentes, aplicando lo establecido en los procedimientos internos y en la normativa vigente y demás normas que las adicionen, modifiquen, reglamenten o complementen. En lo pertinente a la violación de las políticas de seguridad de la información de la AGR, por los funcionarios y contratistas.	Oficina Jurídica - Asuntos disciplinarios	Procedimientos de Asuntos disciplinarios – Proceso Evaluación y Asuntos Disciplinarios -
	Realizar capacitación, entrenamiento y actualización periódica en materia de las políticas, normas y procedimientos de Seguridad y Privacidad de la Información. Lo anterior de acuerdo con el análisis de necesidades realizado por el grupo TIC – AGR	Dirección Talento Humano / Grupo TIC.	Procedimiento de capacitación
	Reportar eventos e incidentes de seguridad y privacidad de la información y apoyar la atención e investigación de estos.	Funcionarios y Contratistas	Incidentes reportados.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Parametrizar en el directorio activo y en el sistema de control de acceso a las instalaciones de la AGR, la inactivación automática de los contratistas, teniendo en cuenta la fecha de terminación del contrato. La inactivación de los usuarios de los sistemas de información que no se autentican con el directorio activo, se debe hacer de forma manual.	Dirección Talento Humano / Grupo TIC.	Políticas del directorio activo y del sistema de control de acceso. Registros de inactivación manual de SI que no se autentican con el directorio activo
	Al recibir las novedades de desvinculación de funcionarios de planta y al terminarse los contratos a los contratistas, se debe: ● Inactivar las credenciales de acceso a plataformas tecnológicas y servicios TIC. ● Cambiar las contraseñas de buzones que pertenecen cuentas de correo genéricas. ● Realizar copia de respaldo de información almacenada en aplicaciones de Drive, herramientas	Dirección Talento Humano Grupo TIC. Recursos Físicos	CAU (Centro de atención al usuario) Sistema de control de Acceso físico.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	colaborativas y del equipo de cómputo. ● Almacenar los activos tangibles e intangibles de información devueltos por funcionario o contratista. ● Recibir el carné y prendas institucionales, si aplica. ● Cancelar el acceso físico a las instalaciones de la AGR.		
	Devolver los activos de información de la AGR que estén en su posesión/responsabilidad al supervisor del contrato, una vez finalizado el contrato o la vinculación con su cargo, según lo estipulado en el procedimiento de desvinculación.	Funcionarios y Contratistas	Procedimiento de desvinculación de la entidad. Soporte de cumplimiento de obligaciones contractuales.

1.3 Política control de accesos.

1.3.1 Objetivo:

Garantizar que la información, las áreas de procesamiento de información, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información de la Auditoría General de la República (AGR) estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.

1.3.2 Alcance:

La presente política aplica para los servidores públicos y contratistas de la AGR que tengan acceso a los sistemas de información, áreas de procesamiento de información, redes de datos y recursos de las plataformas tecnológicas.

1.3.3 Política:

Deben establecerse medidas de control de acceso a nivel de red, sistema operativo, bases de datos, sistemas de información y servicios de T.I. Los controles de acceso deben ser conocidos por todos los funcionarios de la entidad y limitar el acceso hacia los activos de información de acuerdo a lo establecido por el perfil de cargo u obligaciones a desarrollar.

1.3.4 Lineamientos Requisitos del negocio para el control de acceso.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente	Al recibir novedades de planta de funcionarios y contratos se debe realizar el procedimiento correspondiente de acceso a la red.	Dirección Talento Humano / Grupo TIC	procedimiento creación de usuarios. CAU (Centro de atención al usuario)
	Para generar acceso tanto físico como lógico a proveedores como contratistas, el supervisor del contrato debe realizar la solicitud	Supervisores contratos / Grupo TIC	CAU (Centro de atención al usuario)
	Se deben asignar los privilegios de red correspondientes según perfil del cargo u obligaciones a realizar específicas.	Grupo TIC	Procedimiento creación de usuarios. Obligaciones contractuales

1.3.5 Lineamientos gestión de accesos de usuario

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Se debe implementar un proceso formal de registro y de cancelación de registros de usuarios, para posibilitar la asignación de los derechos de acceso	Se debe llevar registro de cuentas de usuario donde se vincula o identifica al usuario	Grupo TIC	Reporte de Directorio activo
	Se deben desactivar el usuario automáticamente o de forma inmediata cuando el funcionario o contratista se desvinculan de la entidad.	Grupo TIC	CAU (Centro de atención al usuario) Directorio Activo.
Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	Autorización del propietario del sistema, datos o servicio de información para el uso de estos activos.	Líder del proceso /Grupo TIC	Procedimiento creación de usuarios. CAU (Centro de atención al usuario)

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Asignación de los roles correspondientes según el perfil asociado	Grupo TIC Administradores de los sistemas de información	Procedimiento creación de usuarios. CAU (Centro de atención al usuario)
	Se modifican los accesos de usuarios que han cambiado de función o puesto de trabajo si procede	Dirección Talento Humano / Grupo TIC	Procedimiento creación de usuarios. CAU (Centro de atención al usuario)
	Se eliminan los accesos de usuarios que han abandonado la organización o ya no desempeñan algún rol en los sistemas de información	Grupo TIC	Sistemas de información CAU (Centro de atención al usuario)

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares	Revisar derechos de acceso a la terminación de empleo o cambios en la organización	Administradores aplicaciones y sistemas de información	Sistemas de información Aplicaciones

1.3.6 Lineamientos control de acceso a sistemas y aplicaciones

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso	Se deben utilizar menús para controlar el acceso a las distintas funciones	Grupo TIC (Equipo de desarrollo)	Sistemas de información Procedimiento desarrollo de software

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Se debe controlar el uso de las funcionalidades por medio de perfiles y roles	Grupo TIC (Equipo de desarrollo)	Sistemas de información Procedimiento desarrollo de software
	Determinar qué datos son accesibles según perfiles y roles	Grupo TIC (Equipo de desarrollo)	Sistemas de información Procedimiento desarrollo de software Inventario activos de información
Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Se debe corroborar la entidad del usuario, cuando la información lo amerite se debe controlar el acceso con medidas adicionales físicas y lógicas	Grupo TIC (Equipo de desarrollo)	Sistemas de información Procedimiento desarrollo de software Inventarios activos de información
	El procedimiento de inicio de sesión no debe mostrar los menús correspondientes de la aplicación hasta que el inicio de sesión haya tenido éxito, se deben evitar mostrar mensajes de ayuda que den pistas a los usuarios no	Grupo TIC (Equipo de desarrollo)	Sistemas de información Procedimiento desarrollo de software

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	deseados, registrar intentos fallidos y hacer que los administradores conozcan esta información.		
	El centro de datos no puede anunciar su nombre en el exterior del edificio.	Grupo TIC	
	Las sesiones inactivas deben ser dependientes del tiempo, cerradas después de un cierto tiempo o un cierto tiempo inactivo	Grupo TIC (Equipo de desarrollo)	Sistemas de información Procedimiento desarrollo de software
Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Deben aplicar contraseñas de calidad, rechazar contraseñas débiles, requerir confirmación y, si se emiten con el usuario, forzar el cambio de las contraseñas en el primer inicio de sesión.	Grupo TIC (Equipo de desarrollo)	Sistemas de información Procedimiento de infraestructura Procedimiento desarrollo de software

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Se deben establecer cambios de contraseñas de forma periódica, además de registrar todas las contraseñas y rechazar contraseñas similares utilizadas anteriormente. El almacenamiento de contraseñas debe mantenerse separado de los sistemas en los que se encuentran las aplicaciones.	Grupo TIC (Equipo de desarrollo)	Sistemas de información Procedimiento de infraestructura Procedimiento desarrollo de software
Se debe restringir el acceso a los códigos fuente de los programas	Controles para mantener registros de la salida y de auditoría de los cambios realizados en el código	Grupo TIC (Equipo de desarrollo)	Sistemas de información Procedimiento desarrollo de software
	El desarrollo debe estar sujeto a los ambientes correspondientes antes del lanzamiento a producción	Grupo TIC (Equipo de desarrollo)	Sistemas de información Procedimiento desarrollo de software

1.4 Políticas de seguridad física y de entorno.

1.4.1 Objeto:

Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la Auditoría General de la República.

1.4.2 Alcance:

Lo definido en la presente guía política aplica para el control de acceso físico a las áreas seguras dentro de las cuales se encuentran el centro de datos, centros de cableado, dirección financiera, archivo y entrega de correspondencia, las cuales deben contar con mecanismos de protección física y controles de acceso adecuados para la protección de la información de la Auditoría General de la República.

1.4.3 Lineamientos de áreas seguras.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	Realizar el inventario y señalizar las áreas seguras de acuerdo con el inventario establecido.	Dirección Recursos Físicos Grupo TIC	Inventario áreas seguras
	El perímetro de seguridad de las instalaciones de la AGR o de las áreas seguras debe ser físicamente sólido (no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Todas las puertas que comunican con el exterior deben ser adecuadamente	Dirección Recursos Físicos Grupo TIC	

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, biométricos, tarjetas lectoras, etc., estás deben permanecer cerradas y cuando no haya personal deben tener llave permanente		
	El perímetro de seguridad de las áreas seguras debe contar con vigilancia mediante CCTV, contar con sistemas de control de acceso al centro de datos y centros de cableado. Las cámaras no podrán apuntar directamente a la captura de información dentro de estas áreas	Grupo TIC	Formato -Ingreso y Salida al Centro de Datos y Centros de Cableado Registros de CCTV
	Mantener organizado e identificado el cableado en los racks de los centros de cableado y centro de datos	Grupo TIC	Informes de mantenimiento de centros de cableado.
Las áreas seguras se deberían proteger mediante controles de entrada, apropiados para asegurar que solamente se permite el acceso a personal autorizado	Deshabilitar o modificar de manera inmediata, los privilegios de acceso físico y a las áreas seguras, en los eventos de desvinculación o ausencia transitoria, lo anterior de acuerdo con las novedades de planta y el proceso de contratación, de acuerdo con la	Grupo TIC	CAU (Centro de atención al usuario)

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Política de Seguridad de los Recursos Humanos.		
	Llevar el registro del acceso a las áreas seguras (centros de datos y centros de cableado). **Nota 1:** El data center externo se rige por las normas y políticas establecidas por el operador de collocation. **Nota 2:** Todo el personal que ingrese al data center y centros de cableado deberá portar identificación visible. **Nota 3:** Cuando se trate de personal externo, deberá estar acompañado por quien sea autorizado, éste se hará responsable de la estadía del personal	Grupo TIC	Formato Ingreso y Salida al data center y Centros de Cableado
Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	Borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se deben dejar documentos o notas escritas en los espacios al finalizar las reuniones, ni encima de los escritorios.	Funcionarios y contratistas AGR	N/A

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Garantizar que los visitantes se encuentren acompañados de un funcionario de la AGR, cuando se encuentren en las oficinas o áreas seguras donde se maneje información, que sean presentados a los funcionarios del área si su permanencia será por más de 1 día.	Funcionarios y contratistas AGR	N/A
	Todos los funcionarios deben portar su carné en un lugar visible mientras permanezca dentro de las instalaciones de la AGR	Funcionarios y contratistas AGR	N/A
	Supervisar las actividades de limpieza y mantenimientos en las áreas seguras, especialmente: Data Center y centros de cableado, brindando capacitación al personal de limpieza acerca de las precauciones mínimas a seguir durante el proceso de limpieza, adicionalmente se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.	Grupo TIC	N/A
Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes	Elaborar e implementar los planes de contingencia, de emergencia y de continuidad del negocio.	Grupo TIC Procesos Misionales	Plan de contingencia y continuidad del negocio

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Mantener libre de objetos o elementos que no sean propios en la operación en el data center y centros de cableado	Grupo TIC	N/A
	Asegurar que el data center y centros de cableado, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones o incendios.	Grupo TIC Dirección Recursos Físicos	N/A
	Proveer las condiciones físicas y medioambientales necesarias como sistemas de control temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia, para certificar la protección y correcta operación de la gestión de la información y de los recursos de la plataforma tecnológica. Estos sistemas se deben monitorear de manera permanente.	Grupo TIC Dirección Recursos Físicos	Registro y monitoreo de aires acondicionados

1.4.4 Lineamientos Equipos

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte cuando sea necesario.	Grupo TIC	Contratos de mantenimiento y soporte.
	Asegurar que la plataforma tecnológica (Hardware, software y comunicaciones) cuente con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.	Grupo TIC Recursos Físicos	N/A
Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Asegurar la protección de los equipos de cómputo contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos.	Grupo TIC Recursos Físicos	Suministro de energía interrumpible (UPS) Planta eléctrica
	Los equipos de UPS deben inspeccionarse periódicamente para asegurar que tienen la capacidad requerida y se deben probar de conformidad con las recomendaciones del fabricante o proveedor.	Grupo TIC Recursos Físicos	Mantenimiento y soporte.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Los interruptores de emergencia deben ubicarse cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica.	Grupo TIC Recursos Físicos	Interruptores de emergencia.
El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño	Los cables de potencia deben estar separados de los cables de comunicaciones para evitar interferencia	Grupo TIC Recursos Físicos	Informes de mantenimiento preventivo y correctivo
	Asegurar que los centros de cableado y/o cuarto eléctrico tengan las condiciones físicas y medioambientales	Grupo TIC Recursos Físicos	Informes de mantenimiento preventivo y correctivo

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar que se les efectúe mantenimiento a los equipos adecuadamente con el objeto de garantizar su disponibilidad e integridad continua.	Grupo TIC	Plan - Informes de mantenimiento preventivo y correctivo
	Sólo los funcionarios o contratistas de TIC autorizado pueden brindar mantenimiento y llevar a cabo reparaciones en los equipos	Grupo TIC	Plan - Informes de mantenimiento preventivo y correctivo
Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	Autorizar el retiro de los equipos, la información o el software de la AGR. Ningún equipo de cómputo, información o software debe ser retirado de la AGR sin una autorización formal.	Recursos Físicos	Formato de retiro de equipos.
	Realizar periódicamente inspecciones para detectar el retiro no autorizado de equipos, información o el software de la AGR	Grupo TIC Recursos Físicos	Formato de retiro de equipos.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Se deberían 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	Asegurar que los equipos que se encuentran sujetos a traslados físicos fuera de la AGR posean pólizas de seguro que cubran los diferentes riesgos que puedan presentar.	Recursos Físicos	Pólizas
	Asegurar que los equipos portátiles no estén a la vista en el interior de los vehículos. En caso de viaje siempre se debe llevar como equipaje de mano.	Funcionarios y contratistas AGR	N/A
	Informar inmediatamente a la dirección de Recursos Físicos y al grupo TIC en caso de pérdida o robo de un equipo portátil, debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de esta.	Funcionarios y contratistas AGR	N/A
	Asegurar con una guaya los equipos portátiles cuando se encuentren desatendidos, dentro de la AGR	Funcionarios y contratistas AGR	N/A

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Se deberían 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 reutilización.	Realizar la copia de respaldo de la información que se encuentre almacenada en los equipos de cómputo. Cuando un equipo de cómputo sea reasignado o dado de baja, posteriormente, debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.	Grupo TIC	Copias de respaldo de los equipos de cómputo. Registros de borrado seguro de la información y del software instalado.
Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	Cerrar las sesiones activas cuando hayan terminado su trabajo y bloquear la pantalla cuando se ausenta de su puesto de trabajo. Salir de las aplicaciones o	Funcionarios y contratistas AGR	N/A

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	servicios de red cuando ya no los necesiten.		

1.5 Política de seguridad de las operaciones

1.5.1 Objetivo:

Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información de la AGR.

1.5.2 Alcance:

Esta guía de política de seguridad de las operaciones aplica para el grupo TIC de la AGR, quienes deben preparar procedimientos documentados para las actividades operacionales asociadas: Gestión del cambio, gestión de capacidad, separación de ambientes, códigos maliciosos

1.5.3 Lineamientos Procedimientos operacionales y responsabilidades.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten	Documentar, actualizar, publicar y socializar los procedimientos de operación.	Grupo TIC	Procedimientos de la operación publicados en SGC

Se deberían 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.	Efectuar todos los cambios a la infraestructura informática y/o servicios de acuerdo con los lineamientos internos	Grupo TIC	Procedimiento Gestión del Cambio
	Llevar una trazabilidad de cambios solicitados y gestionados.	Grupo TIC	CAU (Centro de atención al usuario)
	Especificar en qué momento existen cambios de emergencia en la cual se debe asegurar que los cambios se apliquen de forma rápida y controlada	Grupo TIC	Procedimiento Gestión del Cambio
	Planear los cambios sobre sistemas de información para asegurar que se cuentan con todas las condiciones requeridas para ejecutarlos de una forma exitosa y se debe involucrar e informar a los colaboradores o terceros que por sus funciones tienen relación con el sistema de información	Grupo TIC	Procedimiento Gestión del Cambio CAU (Centro de atención al usuario)
	Especificar en el procedimiento de Gestión de Cambios los canales autorizados para la recepción de solicitudes de cambios.	Grupo TIC	Procedimiento Gestión del Cambio

	Evaluar los impactos potenciales que podría generar un cambio a la aplicación previo a su aplicación, incluyendo aspectos funcionales y de seguridad de la información, estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.	Grupo TIC	Procedimiento Gestión del Cambio
	Probar los cambios realizados sobre sistemas de información para asegurar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente	Grupo TIC	Procedimiento de desarrollo
	Establecer y aplicar el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, como actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad de los sistemas de información y componentes que los soportan, tales como el sistema operativo o cambios en hardware.	Grupo TIC	Procedimiento Gestión del Cambio
	Disponer de un plan de roll-back en la aplicación de cambios, que incluyan las actividades a seguir para abortar los cambios y volver al estado anterior.	Grupo TIC	Procedimiento Gestión del Cambio

Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura	Realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica de la AGR. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, anchos de banda, internet y tráfico de las redes de datos, entre otros.	Grupo TIC	Plan de capacidad Procedimiento Gestión de Capacidad
Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Proveer los recursos necesarios que permitan la separación de ambientes de Desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de pruebas y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.	Grupo TIC	Plan de capacidad Procedimiento infraestructura
	Establecer y mantener ambientes separados de pruebas y producción, dentro de la infraestructura de	Grupo TIC	Procedimiento de desarrollo

	desarrollo de sistemas de información.		
	Seguir un procedimiento formal para el paso de software, aplicaciones y sistemas de información de un ambiente a otro (desarrollo, pruebas y producción), donde se establecen las condiciones a seguir para alcanzar la puesta en producción de un sistema nuevo o la aplicación de un cambio a uno existente.	Grupo TIC	Procedimiento de desarrollo Procedimiento Gestión del cambio
	No se deben realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción	Grupo TIC	Procedimiento de desarrollo Procedimiento Gestión del cambio
	No se deben utilizar datos reales del ambiente de producción, en los ambientes de desarrollo y pruebas sin antes haber pasado por un proceso de ofuscamiento	Grupo TIC	Procedimiento de desarrollo Procedimiento Gestión del cambio
	Identificar claramente las interfaces de los sistemas para poder determinar a qué instancia se está realizando la conexión	Grupo TIC	Procedimiento de desarrollo
	Identificar claramente los ambientes, para evitar así confusiones en la aplicación de tareas o en la ejecución de procesos propios de cada uno	Grupo TIC	Procedimiento de desarrollo

	Informar y consultar con el(los) proceso (s) o dependencias propietario(s) de la información los cambios a sistemas en producción que involucren aspectos funcionales.	Grupo TIC	Procedimiento Gestión del Cambio

1.5.4 Lineamientos protección contra códigos maliciosos.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Asegurar que la infraestructura de procesamiento de información de la AGR, cuente con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.	Grupo TIC	Consola Antivirus.
	Restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores de la AGR, de manera que se reduzca el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica y los servicios que se ejecutan en la misma.	Grupo TIC	Consola Antivirus.
	Administrar el antivirus para proteger a nivel de red y de estaciones de trabajo, contra virus y código malicioso.	Grupo TIC	Consola Antivirus.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Monitorear y supervisar todos los equipos conectados a la red	Grupo TIC	Herramientas de monitoreo.
	Monitorear las comunicaciones y/o la información que se generen, comuniquen, transmitan o transporten y almacenen en cualquier medio, en busca de virus o código malicioso. Si se identifica virus o código malicioso y este no puede ser eliminado, la información será borrada.	Grupo TIC	Firewall
	Mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, etc.	Grupo TIC	Plan de actualizaciones. Monitoreo de actualizaciones
	Contar con controles para analizar, detectar y restringir el software malicioso que provenga de descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc.	Grupo TIC	Consola Antivirus.
	Implementar soluciones lógicas (antivirus) y físicas (dispositivos perimetrales) que garanticen la protección de la información de la AGR de posibles ataques internos o externos y que impidan el acceso no autorizado a la red, las cuales deben permitir: Lógicas:	Grupo TIC	Consola Antivirus. Dispositivos Perimetrales

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	● Detección de ataques en el momento que están ocurriendo o poco después. ● Auditoría de configuraciones y vulnerabilidades de los sistemas. ● Descubrir sistemas con servicios habilitados que no deberían de tener, mediante el análisis del tráfico y de los logs. ● Análisis de comportamiento anormal. Si se detecta una conexión fuera de hora, reintentos de conexión fallidos y otros, existe la posibilidad de que se esté en presencia de una intrusión. ● Un análisis detallado del tráfico y los logs puede revelar una máquina comprometida o un usuario con su contraseña al descubierto. ● Automatizar tareas como la actualización de reglas, la obtención y análisis de logs, la configuración de Firewall.		
	Instalar el único servicio de antivirus autorizado en la AGR, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques de virus, spyware y otro tipo de software malicioso.	Grupo TIC	Consola Antivirus CAU (Centro de atención al usuario)
	Llevar a cabo actividades o estrategias de sensibilización a los funcionarios y contratistas, con el fin de generar una cultura de seguridad de la información, incluyendo la apropiación sobre la protección contra códigos maliciosos	Grupo TIC	Soporte de capacitación

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Manejar el antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.	Funcionarios y Contratistas AGR	N/A
	No podrán desactivar o eliminar los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.		N/A
	Verificar que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.		N/A
	Notificar si sospechan o detectan alguna infección por software malicioso, deben notificar a la mesa de ayuda de tecnología.		CAU (Centro de atención al usuario)
	Destruir los archivos o mensajes, que le haya sido enviado por cualquier medio provisto por la AGR, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los		N/A

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	archivos adjuntos, el usuario debe reenviar el correo a la cuenta establecida para ello.		

1.5.5 Lineamientos copias de respaldo.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Se deberían 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.	Definir un procedimiento formal de administración y control de copias de respaldos que permita conocer qué información está respaldada y almacenada y donde se encuentra alojada.	Grupo TIC	Documento de Políticas de Back Up
	Configurar la herramienta de ejecución de copias de respaldo para que automáticamente registre el éxito o errores en la ejecución.	Grupo TIC Proveedor	
	Verificar periódicamente, la integridad de las copias de respaldo que se están almacenando, con el fin de preservar la integridad y disponibilidad de la información.	Grupo TIC	Documento de Políticas de Back Up

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Determinar junto a los propietarios de la información (directores, Lideres, Coordinadores de áreas) los requerimientos para respaldar la información y los datos en función de su criticidad, para lo cual se debe elaborar y mantener el inventario de activos de Información	Grupo TIC	Documento de Políticas de Back Up Matriz activos de información
	Efectuar las copias de información de los servidores, cada vez que se realice un cambio significativo en los sistemas operativos o configuraciones básicas	Grupo TIC	CAU (Centro de atención al usuario)
	Probar los procedimientos de restauración, para asegurar que son efectivos, que pueden ser ejecutados en los tiempos establecidos y que la información estará disponible en el evento que se requiera para su utilización en casos de emergencia	Grupo TIC	Plan restauración copia de respaldo
	Retener los activos de información de la AGR de acuerdo con las políticas de Backup y con lo establecido en las TRD	Grupo TIC	Documento político de back up TRD
	Realizar las copias de respaldo en horario no hábil, lo cual será verificado a través de procesos automáticos	Grupo TIC	Ejecución Back Up

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	El dueño de los activos de información es responsable de definir claramente el periodo de retención de respaldos	Líderes de procesos	Documento político de back up TRD
	Realizar los respaldos de información personal almacenada en los equipos asignados	Funcionarios y Contratistas AGR	N/A
	Almacenar toda la información relevante a sus funciones en el Drive o equivalente suministrado por la AGR		Drive
	Ningún funcionario ni contratistas de la AGR puede realizar copias de respaldo en sus dispositivos de almacenamiento removibles personales, ya que esto puede ser denominado fuga de información.		N/A
	Almacenar la información crítica asociada con su labor en el servidor de archivos establecido para asegurar que la información está siendo respaldada.		*Docunet*

1.5.6 Lineamientos registro y seguimiento.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del	Configurar la infraestructura, servidores, sistemas, bases de datos, para que queden registrados todos los accesos	Grupo TIC	Logs de infraestructura

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
usuario, excepciones, fallas y eventos de seguridad de la información	de los funcionarios y contratistas de la AGR a los sistemas, redes de datos y aplicaciones. Fecha y hora en que se producen los eventos		
	Habilitar los logs de eventos requeridos y estos deben ser revisados con regularidad.	Grupo TIC	Logs de infraestructura
Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado	Asegurar que los controles estén dirigidos a proteger contra cambios no autorizados de la información del registro y contra problemas con la instalación de registro, inclusive: a) alteraciones a los tipos de mensaje que se registran; b) archivos log que son editados o eliminados; c) se excede la capacidad de almacenamiento del medio de archivo log, lo que da como resultado falla en el registro de eventos, o sobreescritura de eventos pasados registrados	Grupo TIC	

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	Registrar todas las actividades de operación realizadas por los administradores de la infraestructura de procesamiento de información de la AGR	Grupo TIC	Cuentas de administración del directorio activo
	Los administradores de la infraestructura tecnológica y de procesamiento de información de la AGR deben tener asignada una cuenta de usuario exclusiva, a través de la cual se realizarán las actividades de administración y debe ser entregada a través de un proceso formal. Las credenciales de acceso de los administradores del sistema deben custodiarse aplicando un protocolo de seguridad.	Grupo TIC	Acta de entrega de funciones de administrador.
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	Garantizar que todos los relojes de la infraestructura de procesamiento de información de la AGR estén sincronizados con la hora legal colombiana	Grupo TIC	Configuración infraestructura

1.5.7 Lineamientos control de software operacional.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	Instalar y/o configurar todos los servidores conectados a la Red por medio del grupo TIC	Grupo TIC	Control de cambios
	Asegurar que los servidores que proporcionen servicios a través de la red e internet: • Funcionen 24 horas del día los 365 días del año. (exceptuando el tiempo para los mantenimientos programados) • Reciban mantenimiento preventivo mínimo dos veces al año o Reciban mantenimiento semestral que incluya depuración de logs. • Reciban mantenimiento anual que incluya la revisión de su configuración. • Sean monitoreados. • Valorar la necesidad de actualización o instalación.	Grupo TIC	Plan de mantenimientos Reporte de monitoreo

	Configurar los servicios hacia internet sólo a través de los servidores autorizados.	Grupo TIC	CAU (Centro de atención al usuario)

1.5.8 Lineamientos Gestión de vulnerabilidades técnicas.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Se debería 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	Realizar mínimo una vez al año una revisión de vulnerabilidades técnicas a los sistemas de información críticos y misionales por medio de ethical hacking	Grupo TIC	N/A
	Documentar, informar, gestionar y corregir las vulnerabilidades encontradas, adoptando acciones correctivas para mitigar los hallazgos, minimizar el nivel de riesgo y reducir el impacto.	Grupo TIC	CAU (centro de atención al usuario)
Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Probar y evaluar la aplicación de actualizaciones antes de su instalación y valorar los riesgos asociados, para asegurar que son eficaces y no producen efectos secundarios.	Grupo TIC	Control de cambios

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Restringir a los usuarios finales la instalación de software en los equipos de la AGR	Grupo TIC	
	Establecer y monitorear que la infraestructura tecnológica sea usada exclusivamente para el desempeño laboral, o para el desarrollo de las funciones, actividades y obligaciones acordadas o contratadas	Grupo TIC	
	Realizar de manera periódica una inspección del software instalado en los equipos de la AGR y debe desinstalar el software no autorizado.	Grupo TIC	
	El grupo TIC a través del CAU es responsable de instalar, configurar y dar soporte a los equipos de la AGR.	Grupo TIC	
	El grupo TIC son los autorizados para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales y comerciales	Grupo TIC	

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Sólo está permitido el uso de software licenciado por la AGR y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado por el grupo TIC	Funcionarios y Contratistas AGR	N/A
	Las aplicaciones generadas por la AGR en desarrollo de su misión institucional deben ser reportadas al grupo TIC para su administración.	Funcionarios y Contratistas AGR	

1.5.9 Lineamientos Consideraciones sobre auditorías de sistemas de información

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	Acordar y planificar cuidadosamente los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos, bases de datos, componentes TI y aplicativos de la AGR para minimizar las interrupciones en los procesos.	Grupo TIC	N/A
	Acordar y controlar el alcance de las pruebas técnicas de auditoría	Grupo TIC	

	Realizar fuera de horas laborales las pruebas de auditoría que puedan afectar la disponibilidad del sistema.	Grupo TIC	

1.6 Política de seguridad de las comunicaciones.

1.6.1 Objetivo:

Dar los lineamientos generales para asegurar la protección de la información en las redes y sus instalaciones, mantener la seguridad de la información transferida dentro de la entidad y con cualquier entidad externa

1.6.2 Alcance:

Estos lineamientos deben ser aplicados por todos los funcionarios, contratistas de la AGR.

1.6.3 Gestión de la seguridad de las redes.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones	Administrar y gestionar la red de la AGR	Grupo TIC	Switches Core - Switches borde
	proporcionar recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación del servicio de internet.	Grupo TIC	Contrato con proveedores.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Implementar controles que eviten el ingreso a páginas con código malicioso incorporado o sitios catalogados como peligrosos	Grupo TIC	Firewall.
	Monitorear la funcionalidad de las redes a través del uso de analizadores de red.	Grupo TIC	Herramientas de monitoreo.
	No es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red de la entidad, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por el grupo TIC	Funcionarios y Contratistas AGR	N/A
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	Dar el acceso a internet exclusivamente a través de la red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.	Grupo TIC	Firewall.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
internamente o se contraten externamente.	Utilizar el acceso a la red, Internet, exclusivamente para el desarrollo de sus actividades propias de las funciones desempeñadas en la AGR	Funcionarios y Contratistas AGR	Firewall, Directorio Activo
	Usar la red inalámbrica privada de la AGR, para lo cual necesariamente deberá estar dentro del dominio.	Funcionarios y Contratistas AGR	Redes privadas AGR
	Conectarse única y exclusivamente a la red inalámbrica (Invitados) de la AGR a internet. La red inalámbrica de invitados le permitirá utilizar los servicios de internet, en las zonas de cobertura de la AGR. Para el acceso a la red inalámbrica de propósito especial (VIP), se deberá pedir la autorización para su acceso.	Visitantes	Firewall. Controladora WIFI
	Los usuarios que accedan a través de la red invitados no tendrán acceso a los servicios de red local de la AGR	Visitantes	Firewall. Controladora WIFI

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Separar en las redes los grupos de servicios de información, usuarios y sistemas de información	Establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y buscar que se preserve la confidencialidad, integridad y disponibilidad de la información de la AGR	Grupo TIC	Switches Core - Switches borde
	Establecer mecanismos de autenticación seguros para el acceso a la red.	Grupo TIC	Firewall Aplicaciones de control de acceso
	Separar las redes inalámbricas públicas de las redes internas, para preservar los principios de la seguridad de la información.	Grupo TIC	Firewall. Controladora WIFI

1.6.4 Lineamientos transferencia de información.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Asegurar canales para realizar la transferencia de información entre la AGR y las partes externas, dicha información debe quedar firmada y hacer parte del contrato o convenios que se establezca con los terceros.	Grupo TIC Dirección Jurídica Dirección de Estudios Especiales	Contratos o convenios firmados
	Responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos.	Grupo TIC Dirección Jurídica Dirección de Estudios Especiales	Formato - Acuerdo de Colaboración para Intercambio de Información
Proteger adecuadamente la información incluida en la mensajería electrónica	Proteger adecuadamente la información de la AGR incluida en la mensajería electrónica.	Grupo TIC	Plataforma Google - Gmail
	Asegurar el direccionamiento y transporte correctos del mensaje.	Grupo TIC	Plataforma Google - Gmail
	La confiabilidad y disponibilidad del servicio	Grupo TIC	Plataforma Google - Gmail
	La obtención de aprobación antes de usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información	Grupo TIC	Firewall

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Definir las pautas generales para asegurar un adecuado uso de la Suite de Google (correo electrónico, grupos, drive, calendario, sitios y formularios) por parte de los funcionarios y contratistas de la AGR	Grupo TIC	Plataforma Google - Gmail
	Es obligación de los funcionarios realizar la activación de las respuestas automáticas en el servicio de correo de la Entidad, cuando su ausencia sea mayor a tres (3) días, igualmente, está deberá indicar quién es la persona asignada para cubrir su ausencia. Nota: La persona encargada de cubrir la ausencia debe estar autorizada por parte del jefe inmediato o supervisor del contrato	Funcionarios AGR	Plataforma Google - Gmail
	No es permitido el envío o recepción de archivos que contengan extensiones ejecutables (exe, lnk, bat, com, Dll, etc..) en ninguna circunstancia	Funcionarios y Contratistas AGR	Plataforma Google - Gmail

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Es responsabilidad de cada funcionario y contratista asegurar los destinatarios a los cuales va dirigida una comunicación, si estas son listas de distribución, también debe revisarlas con el fin de evitar compartir información a personas no autorizadas.	Funcionarios y Contratistas AGR	Plataforma Google - Gmail
	Es responsabilidad del usuario reportar un correo electrónico cuando crea que es de dudosa procedencia al grupo TIC, con el fin de que el administrador tome las medidas necesarias para evitar su propagación dentro de la entidad.	Funcionarios y Contratistas AGR	Plataforma Google - Gmail
	Está prohibido el envío de o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que atente con la integridad de las personas.	Funcionarios y Contratistas AGR	Plataforma Google - Gmail

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Los mensajes y la información contenida en los buzones de correo son propiedad de la AGR y cada responsable, el cual debe mantener únicamente los mensajes relacionados con el desarrollo de sus actividades	Funcionarios y Contratistas AGR	Plataforma Google - Gmail
	El único servicio de correo electrónico controlado por la AGR es el asignado directamente por el grupo TIC, el cual cumple con todos los requerimientos técnicos y de seguridad para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso	Funcionarios y Contratistas AGR	Plataforma Google - Gmail
	Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la AGR y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.	Funcionarios y Contratistas AGR	Plataforma Google - Gmail

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Los usuarios de correo electrónico tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los servidores públicos de la entidad y el personal provisto por terceras partes	Funcionarios y Contratistas AGR	Plataforma Google - Gmail
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.	En todos los contratos o convenios de la AGR con terceras partes, que implique un intercambio, uso o procesamiento de información de la AGR, se deben realizar acuerdos de confidencialidad y/o acuerdos de protección de datos sobre el manejo de la información, los cuales deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio.	Grupo TIC Dirección Jurídica Dirección de Estudios Especiales	Contratos o convenios firmados
	Definir claramente el tipo de información que se va a intercambiar entre la AGR y la entidad externa.	Grupo TIC Dirección Jurídica Dirección de Estudios Especiales	Contratos o convenios firmados

1.7 Políticas de adquisición, desarrollo y mantenimiento de sistemas.

1.7.1 Objetivo:

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 sobre redes públicas.

1.7.2 Alcance:

Esta guía política aplica a todos los sistemas de información de la AGR, incluyendo los sistemas de información que prestan servicios sobre redes públicas.

1.7.3 Lineamientos requisitos de seguridad de los sistemas de información

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Apoyar a todas las áreas de la AGR en la adquisición o mejora de aplicativos o software.	Grupo TIC	Procedimiento Gestión del Cambios.
	Identificar los requisitos de seguridad de la información y promover que los contratistas de T.I los cumplan: Las políticas de seguridad de la información y demás - -reglamentación definida por la AGR. Identificación de amenazas de seguridad de la información. Revisiones de incidentes.	Grupo TIC Contratistas T.I	Política de Seguridad de la información y políticas técnicas.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Integrar en la etapa de diseño de los proyectos de sistemas de información la identificación y gestión de los requisitos de seguridad de la información y los procesos asociados	Grupo TIC Contratistas T.I	Documentación de los proyectos de sistemas de información

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Exigir, para la adquisición y mantenimientos en los sistemas de información, las mejores prácticas en el ciclo de vida desarrollo de software SDLC (por su sigla en inglés), entre los cuales están: **1. Fase de requerimientos:** • Controles de autenticación y sesión, los requisitos de autenticación de usuario (Usuarios, Claves, token, doble factor, OTP, entre otros). • Los requisitos para la entrega a producción de servicios tecnológicos. - Manejo adecuado de sesiones - Control de roles y privilegios - Los procesos para conceder acceso y autorización a los usuarios de la AGR al igual que a los usuarios privilegiados (Administradores, súper usuarios o técnicos) mediante la definición de la matriz de roles y privilegios. • Informar a los usuarios y operadores sobre sus deberes y responsabilidades. • Asegurar la asignación de menor privilegio, los usuarios solo deben ser capaces de acceder a los sistemas de información, que por el	Grupo TIC Contratistas T.I	Política de Seguridad de la información, Políticas técnicas. Procedimiento de desarrollo Gestión de cambios.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	desempeño de sus funciones requieran. • Las necesidades de protección de activos de información involucrados, para preservar la disponibilidad, confidencialidad e integridad. **2. Fase de análisis y diseño:** • Acceso a componentes y a la administración del sistema. • Pistas de auditoría. • Gestión de sesiones. • Datos históricos. • Manejo apropiado de errores • Separación de funciones (Segregación de funciones) Las pistas de auditoría no se pueden eliminar, se debe realizar una copia periódicamente para liberar espacio en su almacenamiento primario; su custodia debe ser segura. **3. Fase de implementación y codificación:** • Aseguramiento del ambiente de desarrollo. • Elaboración de documentación técnica. • Codificación segura (Buenas prácticas).		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	• Estilo de programación • Manejo de log de cambios. • Manejo de errores y logs. • Manejo de archivos. • Estandarización y reutilización de funciones de seguridad. • Seguridad en las comunicaciones. • Seguridad en el paso a ambientes de producción. **4. Fase de pruebas** • Control de calidad en controles de seguridad (con y sin credenciales de acceso). • Comprobación de gestión de configuraciones.		

1.7.4 Lineamientos seguridad en los procesos de desarrollo y soporte.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	**1. Análisis – Diseño de Sistemas en la AGR.** Se deben considerar los siguientes aspectos: ● Definir el alcance. ● Especificar los atributos de calidad en seguridad que debe cumplir la arquitectura. ● Especificar los requerimientos. ● Realizar el levantamiento de información. ● Solicitar la Infraestructura que se requiere para los Ambientes de Desarrollo y Prueba.	Grupo TIC Contratistas T.I	Política de Seguridad de la información y políticas técnicas. Documentación de los proyectos de sistemas de información

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	1.1 Requisitos de Seguridad Identificar los objetivos y requisitos de seguridad que se deben contemplar e implementar; estos se determinan de la siguiente forma: • Arquitectura de la aplicación. Plataforma donde correrá la aplicación. • Tipos de datos que se almacenarán, consultarán o transferirán, es decir se debe definir cuáles son confidenciales y/o públicos de acuerdo con la clasificación de información. • Tipos de registro que el sistema debe generar, acceso a los recursos, niveles de privilegios, perfiles de usuario. • Los tipos de acceso a los datos deben ser estructurados de acuerdo con los perfiles definidos, lectura, escritura, modificación y eliminación. • Definir cómo será el modo de autenticación al ingreso al aplicativo, por ejemplo, usuario y contraseñas, tokens, entre otros. En esta etapa es necesario identificar los riesgos del proyecto	Grupo TIC Contratistas T.I	Política de Seguridad de la información y políticas técnicas. Documentación de los proyectos de sistemas de información Procedimiento de desarrollo

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	2. Desarrollo • Contar con ambientes de desarrollo, pruebas y producción y estos deben ser independientes. Estos ambientes deben ser lo más similar posible y con los mismos controles de seguridad, a efectos de prevenir situaciones en las cuales el software desarrollado presente comportamientos distintos y errores en el ambiente de pruebas y producción. • Los desarrolladores deben realizar su trabajo exclusivamente en ambiente de desarrollo, nunca en otros ambientes directamente. • Los nombres de dominio para los ambientes desarrollo, pruebas y producción deben ser diferentes a efectos de evitar confusión durante la ejecución desarrollo, pruebas, y puesta en producción. Es necesario que se tenga instalado el mismo manejador de base de datos y versión en los ambientes de prueba y producción.	Grupo TIC Contratistas T.I	Política de Seguridad de la información y políticas técnicas. Documentación de los proyectos de sistemas de información Procedimiento de desarrollo

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	• Incluir réplicas de todos los componentes con los cuales el software tendrá interoperación en producción incluyendo: otras aplicaciones cliente servidor, bases de datos relacionales, componentes middleware, interfaces, demonios (daemons), procesos personalizados, utilidades FTP y otros.		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Buenas Prácticas de Desarrollo de Software ● Utilizar sistemas de control de versiones y de gestión de configuración. ● Emplear nombres descriptivos, en la declaración de variables, es decir, que hagan alusión a su nombre y no a su tipo. ● Implementar el encapsulamiento en variables globales para privatizar su estado desde fuera del ámbito de la clase, su acceso se pueda realizar por inyección de dependencia en caso de servicio para garantizar el bajo acoplamiento entre estos o, por procedimiento público o protegido para el aprovechamiento y hacer efectivo el monitoreo y seguimiento de fallas, incidentes y errores mediante tracking (auditoría de eventos) o logging (historial de transacciones). ● Inicializar siempre las variables. La aplicación deberá generar y almacenar un log de auditoría sobre	Grupo TIC Contratistas T.I	Política de Seguridad de la información y políticas técnicas. Documentación de los proyectos de sistemas de información Procedimiento de desarrollo

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	las tablas y transacciones críticas, que permita consultar como mínimo: ID de usuario, fecha, hora, tabla modificada, acción ejecutada (creación, modificación, borrado, contenido antes y después de las modificaciones). Si el volumen de datos y la carga transaccional de la aplicación no es muy elevada es aconsejable registrar los valores anteriores y actuales. ● Los comentarios que contengan el código fuente deben ir enfocados a describir la funcionalidad que se está programando, en los bloques de código extenso es recomendable dividirlos e introducir un comentario al principio con el fin de guiar al desarrollador, sería óptimo que exista una línea blanca de separación, estos comentarios no deben ser excesivos, es decir describiendo lo obvio. ● Reutilización de Código Fuente: En lo posible se recomienda la reutilización de código fuente cuya calidad haya sido verificada, ya que la no reutilización de código induce a errores cada vez que se desarrolla un nuevo componente de la solución. En caso de requerir funciones de seguridad específicas		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	es recomendable hacer uso de librerías y/o piezas de código ya construidas para tal fin, con el fin de aprovechar la experiencia de los desarrolladores especializados en estas áreas. ● No excederse con el número de niveles en las instrucciones anidadas. No mezclar datos con código. ● Evitar usar métodos con muchos parámetros, en caso de que sea necesario es recomendable contemplar la creación de una clase que contenga las propiedades requeridas. ● Se deben validar todos los parámetros de las interfaces de programación de aplicaciones (API) exportadas, verificando que sean válidos, esto incluye los datos que parecen ser coherentes pero que están más allá del intervalo de valores aceptado, como los tamaños de búfer excesivos. ● Cuando una funcionalidad se requiera implementar en diferentes aplicaciones se recomienda crear una función, una rutina, un servicio o un componente que sea reutilizable para cualquier aplicación.		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	● Todas las comunicaciones deben ser seguras. ● Evitar generar código a partir de valores ingresados por el usuario. ● Utilizar *Stored Procedures* en lugar de sentencias SQL dinámicas.		
Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	• Documentar y hacer cumplir los procedimientos formales de control de cambios que se tienen definidos por la AGR, para asegurar la integridad del sistema, las aplicaciones y los productos, desde las primeras etapas de diseño a través de todos los esfuerzos de mantenimiento posteriores. Este proceso debe incluir: ● Una valoración de riesgos de seguridad Análisis de los impactos de los cambios y la especificación de los controles de seguridad. ● El uso de un sistema de gestión de versiones, que permite recuperar versiones específicas cuando se requiera.	Grupo TIC Contratistas T.I	Procedimiento Gestión de Cambios. Procedimiento de Desarrollo

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	• Exigir que en los nuevos sistemas y cambios importantes a los sistemas existentes se ejecute un proceso formal de documentación, especificación, pruebas, control de calidad y gestión de la implementación.		
Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas de la AGR, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad.	Garantizar que cuando se cambian las plataformas de operación (sistemas operativos, bases de datos y aplicaciones), se revisan las aplicaciones críticas del negocio, y se prueban para asegurar que no haya impacto adverso en las operaciones o seguridad de la AGR. Esto debe comprender: ● Revisar los procedimientos para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones. ● Garantizar 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.	Grupo TIC Contratistas T.I	Procedimiento Gestión de Cambios.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
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.	Controlar las modificaciones al software de la AGR, las cuales se deben limitar a los cambios necesarios. En donde un software necesite modificaciones, se deben considerar los siguientes puntos: ● Se debe contar con sistema de gestión de versiones que permite recuperar versiones previas en caso de ser necesario. ● El riesgo de que los procesos se vean comprometidos; Tener el consentimiento del proveedor (vendedor). Obtener del proveedor (vendedor) los cambios requeridos, a medida que se actualiza el programa estándar. ● El impacto, si la AGR llega a ser responsable del mantenimiento futuro del software como resultado de los cambios ● La compatibilidad con otro software en uso en la AGR	Grupo TIC Contratistas T.I	Procedimiento Gestión del Cambios.
	● Implementar un plan de gestión de actualizaciones de software para asegurar que se instalen las actualizaciones de aplicaciones y de parches	Grupo TIC Contratistas T.I	Plan de actualizaciones

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	aprobados más recientes para todo el software autorizado.		
	Exigir que todos los cambios se prueben y documenten completamente, de manera que se puedan aplicar nuevamente, si es necesario, a futuras actualizaciones de software.	Grupo TIC Contratistas T.I	Procedimiento de desarrollo Procedimiento Gestión del Cambios.
Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información	Establecer, documentar y aplicar lineamientos de construcción de sistemas de información seguros, basados en principios de desarrollo seguro en la AGR. Tener en cuenta los siguientes principios de construcción de sistemas de información seguros: ● Partir siempre de un modelo de permisos mínimos, es mejor ir	Grupo TIC Contratistas T.I	Procedimiento de desarrollo Procedimiento Gestión de Cambios.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	escalando privilegios por demanda de acuerdo con los perfiles establecidos en las etapas de diseño. ● Todos los accesos que se hagan a los sistemas deben ser validados. ● Si se utiliza un lenguaje que no sea compilado, asegurarse de limpiar el código que se pone en producción, para que no contenga rutinas de pruebas, comentarios o cualquier tipo de mecanismo que pueda dar lugar a un acceso indebido. ● Si se utiliza un lenguaje compilado, se debe garantizar que la compilación se realiza utilizando las mejores optimizaciones disponibles y que no se incluya información para depuración. ● La seguridad se debe incluir en el diseño de todas las capas de arquitectura (negocio, datos, aplicaciones y tecnología) equilibrando la necesidad de seguridad digital, con la necesidad de accesibilidad. ● Cualquier funcionalidad, campo, botón o menú nuevo debe agregarse de acuerdo con los requerimientos de diseño. De esta forma se evita tener porciones de		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	código que resultan siendo innecesarias. ● Cualquier cambio que se haga debe quedar documentado, esto facilitará modificaciones futuras. ● Los principios y los procedimientos de construcción establecidos se deben revisar con regularidad para asegurar que están contribuyendo efectivamente a mejorar los estándares de seguridad dentro del proceso de construcción de software de la AGR. ● Haber pasado por un proceso completo de pruebas (técnicas, funcionales, seguridad, etc.) y certificación los sistemas de información de la AGR, antes de ser liberados a producción en un ambiente dedicado para tal fin.		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
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	Exigir a los proveedores e ingenieros del grupo TIC en los desarrollos de software para la AGR, que deben contar con ambientes independientes tales como: • Desarrollo, pruebas y producción, estos deben contemplar controles físicos y de acceso lógico para asegurar la separación de estos. (Aplica para sistemas de información nuevos o existentes)	Grupo TIC Contratistas T.I	Procedimiento de desarrollo Procedimiento Gestión de Cambios.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Los controles que se deben tener en cuenta: ● Los datos almacenados en el ambiente de producción no deben ser utilizados para las actividades de desarrollo o pruebas. ● Los datos utilizados en los ambientes de desarrollo, pruebas, no deben ser los utilizados en el ambiente de producción. ● Habilitar solo los módulos, servicios, protocolos y aplicaciones que sean necesarias para el buen funcionamiento del sistema de información. Aquellos que no se utilicen deberán ser deshabilitados. El desarrollador es responsable de documentar cuáles son estrictamente necesarios para el correcto funcionamiento del aplicativo. ● Verificar que los aplicativos cuenten con las últimas versiones estables, tanto a nivel de software como de sistema operativo, parches de		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	seguridad, servidor de aplicaciones, base de datos, etc., antes del despliegue. ● Verificar que no se pueda listar los directorios de la aplicación. o Verificar que en el servidor no se encuentren instalados módulos, extensiones, programas por defecto y que no serán usados por la aplicación. ● Controlar para que los usuarios no tengan acceso a aquellos archivos de configuración o a directorios sensibles que no puedan ser eliminados. Solo usuarios con privilegios o autorizados deberán tener acceso. ● Controlar para que todos los usuarios de la aplicación y el software que se ejecuten en el servidor (base de datos, sftp, apache, iis, tomcat, etc.) tengan los mínimos privilegios sobre el sistema. ● Garantizar que no se permita la transferencia de archivos con configuraciones del sistema a los usuarios. ● Controlar si la aplicación requiere que el usuario adjunte archivos, verificar que solo este		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	permitido el envío de documentos con extensiones específicas, por ejemplo: doc, docx, pdf, zip. No permitir que el usuario adjunte archivos con extensiones asp, txt, php, jsp, exe, etc. ● Controlar para que los archivos que son enviados por el usuario no sean almacenados en el mismo entorno de trabajo de la aplicación, se recomienda guardarlos en un dispositivo aislado. ● Controlar y de ser posible solo permitir el cargue de archivos .pdf a los sistemas de información y, en la medida de lo posible, no deben incluir scripts. ● Controlar para que los archivos transferidos al servidor por el usuario no se almacenen con permisos de ejecución, sólo de lectura. ● No utilizar rutas específicas en los parámetros o variables, se recomienda, utilizar índices que internamente se asocien a directorios o rutas predefinidas. utilizar protocolos seguros, tales como SSH, SFTP, FTPS, VPN		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	SSL, IP SEC, etc. Para la comunicación y transferencia de archivos. ● Todos los sistemas que implementen Web Services dentro de su funcionamiento, deben contar con mecanismos de seguridad adecuados. ● Procurar implementar los servicios de interoperabilidad con tecnología REST.		
La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados	● Supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente por la AGR	Grupo TIC Supervisor de contratos	N/A
	Verificar y hacer cumplir por parte del tercero los siguientes puntos en toda la cadena de suministro de desarrollo de software: ● Los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente. ● Los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas. ● Las pruebas de aceptación para determinar la calidad y exactitud de los entregables.	Grupo TIC Supervisor de contratos	

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	● La entrega de evidencias de que se han hecho pruebas suficientes para garantizar que el sistema está protegido contra contenido malicioso intencional y no intencional en el momento de la entrega. ● Aceptar las políticas y procedimientos que se encuentran dentro de este documento. ● Cumplir con el procedimiento de gestión de cambio.		
	Establecer programas de prueba para aceptación y criterios de aceptación relacionados para los sistemas de información nuevos, actualizaciones y nuevas versiones.	Grupo TIC Supervisor de contratos	

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	Se deben tener en cuenta las siguientes consideraciones al realizar pruebas de seguridad: ● Las revisiones de código pueden ser realizadas por terceros contratados para tal efecto, o por personal interno capacitado para hacerlo con el fin de asegurar la idoneidad de quien realiza dicha actividad. ● Puede realizarse a través de herramientas automáticas o mediante técnicas manuales.	Grupo TIC Contratistas T.I	
	Verificar que los aplicativos cuenten con las últimas versiones estables, tanto a nivel de software como de sistema operativo, parches de seguridad, servidor de aplicaciones, base de datos, etc., antes del despliegue.	Grupo TIC Contratistas T.I	

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados	Establecer programas de prueba para aceptación y criterios de aceptación relacionados para los sistemas de información nuevos, actualizaciones y nuevas versiones. Definir y ejecutar las pruebas de aceptación de software a partir de los siguientes elementos: • Requerimientos del usuario. • Requerimientos de sistema. Procesos de negocio.	Grupo TIC Contratistas T.I	Documento Pruebas de aceptación
Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente	Seleccionar, proteger y controlar cuidadosamente los datos de prueba que se utilicen para los desarrollos de sistemas de información en la AGR	Grupo TIC Contratistas T.I	Documento Pruebas de aceptación
	Autorizar específicamente cada copia información operacional a un ambiente de pruebas.	Grupo TIC Contratistas T.I	Documento Pruebas de aceptación

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Evitar el uso de datos operacionales que contengan información de datos personales o cualquier otra información confidencial para propósitos de prueba. Si esta información de datos personales u otra información confidencial se usa para propósitos de las pruebas, todos los detalles y contenido sensible se deben proteger eliminándolos o modificándolos (anonimizar); con previo permiso del responsable o dueño de la información	Grupo TIC Contratistas T.I	Documento Pruebas de aceptación
	La información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas.	Grupo TIC Contratistas T.I	

1.8 Política de seguridad de relación con los proveedores.

1.8.1 Objetivo

Establecer las condiciones para la prestación de los servicios, responsabilidades y controles que ayuden a proteger la información involucrada en las relaciones entre la Auditoría general de la república con sus proveedores, frente a interceptaciones, copia, modificación, divulgación y destrucción no autorizada, que puedan afectar los principios de integridad, disponibilidad y confidencialidad de la información.

1.8.2 Alcance

Esta guía política aplica para todos los proveedores que para la ejecución de su trabajo requieran acceder a la información o infraestructura tecnológica de la Auditoría General de la República.

1.8.3 Lineamientos política de seguridad de la información para las relaciones con los proveedores.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de organización se deben acordar con éstos y se debe documentar	Tener en cuenta los procesos y procedimientos que va a implementar la AGR, al igual que los procesos y procedimientos que debe exigir a sus proveedores que implementara, incluidos: ● La identificación y documentación de los tipos de proveedores, por ejemplo, servicios de TI, utilidades logísticas, servicios financieros, componentes de la infraestructura de TI, a quienes la AGR permitirá acceso a su información. ● La definición de los tipos de acceso a la información que se permitirá a diferentes tipos de proveedores, y el seguimiento y el control del acceso. ● Los requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso, que sirvan como base para los acuerdos con proveedores individuales, con base en las necesidades y requisitos del negocio de la AGR.	Dirección Jurídica Grupo TIC	Políticas técnicas de seguridad de la información

	Identificar y exigir los controles de seguridad de la información a tener en cuenta en el acceso de los proveedores a la información de la AGR	Dirección Jurídica Grupo TIC	Contratos Políticas técnicas de seguridad de la información
	Identificar los tipos de obligaciones aplicables a los proveedores para proteger la información	Dirección Jurídica Grupo TIC	Contratos Políticas técnicas de seguridad de la información
Establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar, o suministrar componentes de infraestructura de TI para la información de la entidad	Establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la AGR	Dirección Jurídica Grupo TIC	Contratos Políticas técnicas de seguridad de la información
	Exigir que, en todos los contratos o acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de la AGR, se deben realizar acuerdos de confidencialidad y/o acuerdos de protección de datos sobre el manejo de la información.	Dirección Jurídica Grupo TIC	Contratos Acuerdo de confidencialidad Políticas técnicas de seguridad de la información

	Incluir en los acuerdos de confidencialidad con los proveedores: ● Asegurar y describir que los requisitos legales y de reglamentación, incluida la protección de datos, los derechos de propiedad intelectual y derechos de autor se cumplan. ● Exigir una lista explícita de personal del proveedor autorizado para tener acceso a la información de la AGR o recibirla de ella, o los procedimientos o condiciones para la autorización, y el retiro de la autorización para el acceso o recibo de información de la entidad por parte del personal del proveedor. ● Monitorear las obligaciones de los proveedores relativas al cumplimiento de los requisitos de seguridad de la organización.	Dirección Jurídica Grupo TIC	Contratos Acuerdo de confidencialidad Políticas técnicas de seguridad de la información
Incluir en los acuerdos con los proveedores los requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	Asegurar que los acuerdos con proveedores incluyan requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	Dirección jurídica Grupo TIC	Especificaciones técnicas de los contratos

	Definir los requisitos de seguridad de la información para aplicar a la adquisición de productos o servicios de tecnología de la información y de comunicaciones, además de los requisitos generales de seguridad de la información para las relaciones con los proveedores.	Dirección jurídica Grupo TIC	Especificaciones técnicas de los contratos

1.8.4 Gestión de la prestación de servicios de proveedores.

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
La organización debe hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan, y que los incidentes y problemas de seguridad de la información se gestionan apropiadamente.	Grupo TIC	

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Gestionar 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, y la revaloración de los riesgos.	Debe considerar los siguientes aspectos: ● Los cambios en los acuerdos con los proveedores. ● Los cambios hechos por la organización para implementar. ● Las mejoras a los servicios ofrecidos en la actualidad. ● El desarrollo de nuevas aplicaciones y sistemas. ● Las modificaciones o actualizaciones a las políticas y procedimientos de la entidad. ● Los controles nuevos o modificados para resolver incidentes de seguridad de la información y mejorar la seguridad.	Grupo TIC	Procedimiento Gestión de Cambios

1.9 Política Gestión de incidentes de seguridad de la información.

1.9.1 Objetivo:

Gestionar adecuadamente todos los incidentes de seguridad de la información reportados en la AGR dando cumplimiento a los procedimientos establecidos.

1.9.2 Alcance:

Esta política aplica para todos los funcionarios y contratistas de la AGR que detecten un evento o incidente de seguridad de la información el cual deben reportar, adecuadamente.

1.9.3 Lineamientos Gestión de incidentes y mejoras en la seguridad de la información

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información	Establecer las responsabilidades en la gestión de incidentes dentro de la seguridad de la información	Grupo TIC	Formato roles y responsabilidades Procedimiento gestión de incidentes
	Definir el procedimiento de atención de incidentes y problemas de seguridad de la información		Procedimiento Gestión de Incidentes
	Dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados		CAU (Centro de atención al usuario)
	Realizar sensibilización a todos los colaboradores y terceros sobre incidentes de seguridad de la información.		Soportes actividades de sensibilización

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Informar sobre los eventos de seguridad de la información a través de los canales de gestión apropiados, tan pronto como sea posible	Reportar de forma inmediata de acuerdo con el procedimiento previsto los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.	Funcionarios y Contratistas	CAU (Centro de atención al usuario) Correo electrónico
Los eventos de seguridad de la información se deben evaluar y decidir si se van a clasificar como incidentes de seguridad de la información	Evaluar cada evento o incidente de seguridad de la información presentado en la AGR, usando la escala de clasificación de eventos e incidentes de seguridad de la información con el fin de poder determinar clasificación y priorización. De acuerdo con el definido en el procedimiento previsto.	Grupo TIC	Registro de categorización del incidente de seguridad de la información
	Registrar los resultados de la evaluación y la decisión para referencia y verificación futuras (Lecciones aprendidas).	Grupo TIC	Informe de Gestión de Incidentes de Seguridad de la Información

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados	Responder a los incidentes de seguridad de la información que se presenten en la AGR, las respuestas deben incluir: ● Recolectar evidencia lo más pronto posible después de que ocurra el incidente. ● Llevar el asunto a una instancia superior, según se requiera. ● 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. ● Tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente. ● Una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto.	Grupo TIC	Informe de Gestión de Incidentes de Seguridad de la Información Soportes de ejecución de acciones.
	Escalar los incidentes a niveles superiores o control interno en caso de que sea requerido.	Grupo TIC	Registro de comunicación

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Usar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la posibilidad o el impacto de incidentes futuros	Documentar todos los incidentes de seguridad de la información reportados en la AGR	Grupo TIC	CAU (centro de atención al usuario)
	Llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos en la AGR	Grupo TIC	Herramienta Bitácora Incidentes
	Desarrollar y seguir procedimientos internos cuando se trata con evidencia para propósitos de acciones legales y disciplinarias	Grupo TIC	Procedimientos y Documentación aplicable

1.10 Políticas de cumplimiento.

1.10.1 Objetivo:

Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad en la AGR, y asegurar que se revisen y actualicen periódicamente, como mínimo una vez al año o cuando se presente una actualización en la normatividad que afecte la seguridad de la información.

1.10.2 Alcance

La guía política de cumplimiento será aplicada por todas las dependencias de la AGR, por todos los colaboradores y contratistas.

1.10.3 Lineamientos Cumplimiento de los requisitos legales y contractuales

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y en el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.	Documentar los controles y las responsabilidades individuales para cumplir estos requisitos estatutarios, reglamentarios y contractuales	Grupo TIC	Formato roles y responsabilidades
	Identificar toda la legislación aplicable a la AGR para cumplir los requisitos de la Auditoría General de la República	Líderes de procesos	Normogramas
	Identificar y documentar explícitamente todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la AGR para cumplirlos y mantenerlos actualizados para cada sistema de información.	Líderes de procesos	Normogramas

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados	Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.		
	Asegurar la protección de cualquier material que se pueda considerar propiedad intelectual, teniendo en cuenta los siguientes lineamientos: ● Publicar una política de cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos. ● Adquirir software solo a través de fuentes conocidas y confiables, para asegurar que no se violen los derechos de autor. ● Mantener conciencia de las políticas para proteger los derechos de propiedad intelectual y notificar la intención de tomar acciones disciplinarias contra el personal que las incumpla. ● Mantener los registros de activos apropiados, e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual.		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	● Mantener prueba y evidencia de la propiedad de las licencias, discos maestros, manuales, etc. ● Implementar controles para asegurar que no se exceda el número máximo de usuarios permitido dentro de cada licencia. ● Llevar a cabo revisiones para verificar que solo hay instalados software autorizado y productos con licencia. ● Definir una política para mantener las condiciones de licencia apropiadas. ● Definir una política para disposición o transferencia de software a terceros. ● No copiar total ni parcialmente libros, artículos, reportajes u otros documentos diferentes de los permitidos por la ley de derechos de autor.		
Proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio	● Proteger los registros (por ejemplo, registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales) contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales.		

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	Clasificar los registros por tipos, por ejemplo, registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales, cada uno con detalles de los períodos de retención y tipo de medio de almacenamiento permisible, por ejemplo, papel, microfichas, medios magnéticos, medios ópticos, almacenamiento en nube. Cualquier llave criptográfica y programas relacionados asociados con archivos permanentes encriptados o firmas digitales, también se deben almacenar de manera segura para posibilitar la desencriptación de los registros durante el tiempo en que están retenidos.		Tabla de retención documental
Asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.	Desarrollar e implementar una política relativa a datos de la AGR, para la privacidad y la protección de datos personales. Esta política se debe comunicar a todas las personas involucradas en el procesamiento de información de datos personales.	Grupo TIC	Política de Tratamiento de Datos Personales

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
	El funcionario incumpla cualquiera de los lineamientos descritos en las Políticas Publicas de Seguridad de la Información, será sancionado disciplinariamente conforme lo establecido en la Ley 734 de 2001 (CDU), Ley 1952 de 2019 (CGD) y Ley 2094 de 202	Grupo Control Disciplinario Interno AGR	Informe de incumplimiento

1.10.4 Lineamientos Revisión de seguridad de la información

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Revisar independientemente a intervalos planificados o cuando ocurran cambios significativos, el enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información	Revisar de forma independiente a intervalos planificados, mínimo una vez al año o cuando ocurran cambios significativos la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información).	Oficina Control interno	procedimiento Auditorías Internas - Control interno

CONTROL	LINEAMIENTOS	INVOLUCRADOS	SOPORTE A LINEAMIENTOS
Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad	Revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad de la información, y cualquier otro requisito de seguridad.	Líderes de procesos	Soportes Revisión por la Dirección
Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información	Revisar periódicamente, mínimo una vez al año, los sistemas de información para determinar el cumplimiento de las políticas y normas de seguridad de la información.	Grupo TIC	Informe de vulnerabilidades

3. Información de contacto.

Cualquier inquietud relacionada con la guía política de cumplimiento de requisitos legales y contractuales, favor remitirla al correo seguridaddelainformacion@auditoria.gov.co

4. Revisión Política.

Esta política debe ser revisada por el grupo de TIC como mínimo una vez al año.

5. Referentes Normativos.

- Norma ISO 27001
- Manual de seguridad y privacidad de la información – Min TIC - Estrategia de Gobierno Digital.

6. Definiciones.

- **MSPI**: Es el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información – MINTIC.

- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- **Disponibilidad:** Acceso y uso de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

- **Copias de respaldo:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

- **Activo de Información:** Es todo aquello que en la entidad es considerado importante o de alta validez para la misma, ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.

- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

- **Carpetas Compartidas:** es básicamente igual que una carpeta normal salvo que su contenido será accesible para todos los usuarios que pertenezcan a un mismo grupo de trabajo.

- **File Server:** Es un servidor de archivos que almacena y distribuye diferentes tipos de archivos informáticos confidenciales o críticos de la AGR.

- **Información confidencial o crítica:** Es aquella información que no se debe circular más allá de las personas que están autorizadas a conocerlas en la AGR

- **AGR**: Auditoría General de la República.

- **CAU**: es el único Centro de Atención al Usuario en donde el grupo TIC presta servicios con la posibilidad de gestionar la atención de requerimientos relacionados con los servicios TIC en la AGR.

- **Drive**: Sitio para almacenamiento virtual en la nube de la información pública de las áreas de la institución.