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

MUNICIPIO DE YONDÓ

ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
CONTROL DE ACCESO									
T.1	**Responsable de SI/Responsable de TICs**	**CONTROL DE ACCESO**		**A.9**	**Componente planificación y modelo de madurez nivel gestionado**			**62**	
T.1.1	Responsable de SI	**REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO**	**Se debe limitar el acceso a información y a instalaciones de procesamiento de información.**	**A.9.1**	Modelo de madurez definido			**70**	
T.1.1.1	Responsable de SI	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	A.9.1.1		PR.DS-5	Revisar que la política contenga lo siguiente: a) los requisitos de seguridad para las aplicaciones del negocio; b) las políticas para la divulgación y autorización de la información, y los niveles de seguridad de la información y de clasificación de la información; c) la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes; d) la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios; e) la gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles; f) la separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso); g) los requisitos para la autorización formal de las solicitudes de acceso; h) los requisitos para la revisión periódica de los derechos de acceso; i) el retiro de los derechos de acceso; j) el ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información de autenticación secreta, en el archivo permanente; k) los roles de acceso privilegiado;	100	
T.1.1.2	Responsable de TICs	Acceso a redes y a servicios en red	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	A.9.1.2		PR.AC-4 PR.DS-5 PR.PT-3	Revisar la política relacionada con el uso de redes y de servicios de red y verificar que incluya: a) las redes y servicios de red a los que se permite el acceso; b) los procedimientos de autorización para determinar a quién se permite el acceso a qué redes y servicios de red; c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y a los servicios de red; d) los medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas); e) los requisitos de autenticación de usuarios para acceder a diversos servicios de red; f) el seguimiento del uso de servicios de red.	40	
T.1.2	Responsable de SI	**GESTIÓN DE ACCESO DE USUARIOS**	**Se debe asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.**	**A.9.2**	Modelo de madurez gestionado cuantitativamente			**27**	
T.1.2.1	Responsable de SI	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	A.9.2.1		PR.AC-1	Revisar el proceso para la gestión y la identificación de los usuarios que incluya: a) Identificaciones únicas para los usuarios, que les permita estar vinculados a sus acciones y mantener la responsabilidad por ellas; el uso de identificaciones compartidas solo se debe permitir cuando sea necesario por razones operativas o del negocio, y se aprueban y documentan; b) deshabilitar o retirar inmediatamente las identificaciones de los usuarios que han dejado la organización; c) identificar y eliminar o deshabilitar periódicamente las identificaciones de usuario redundantes; d) asegurar que las identificaciones de usuario redundantes no se asignen a otros usuarios.	20	

T.1.2.2	Responsable de SI	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	A.9.2.2		PR.AC-1	Revisar el proceso para asignar o revocar los derechos de acceso otorgados a las identificaciones de usuario que incluya: a) obtener la autorización del propietario del sistema de información o del servicio para el uso del sistema de información o servicio; b) verificar que el nivel de acceso otorgado es apropiado a las políticas de acceso y es coherente con otros requisitos, tales como separación de deberes; c) asegurar que los derechos de acceso no estén activados antes de que los procedimientos de autorización estén completos; d) mantener un registro central de los derechos de acceso suministrados a una identificación de usuario para acceder a sistemas de información y servicios; e) adaptar los derechos de acceso de usuarios que han cambiado de roles o de empleo, y retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han dejado la organización; f) revisar periódicamente los derechos de acceso con los propietarios de los sistemas de información o servicios.	20	
T.1.2.3	Responsable de SI	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	A.9.2.3		PR.AC-4 PR.DS-5	Revisar la asignación de derechos de acceso privilegiado a través de un proceso de autorización formal de acuerdo con la política de control de acceso pertinente. el proceso debe incluir los siguientes pasos: a) Identificar los derechos de acceso privilegiado asociados con cada sistema o proceso, (sistema operativo, sistema de gestión de bases de datos, y cada aplicación) y los usuarios a los que es necesario asignar; b) definir o establecer los derechos de acceso privilegiado a usuarios con base en la necesidad de uso y caso por caso, alineada con la política de control de acceso; c) mantener un proceso de autorización y un registro de todos los privilegios asignados. Sólo se debe suministrar derechos de acceso cuando el proceso de autorización esté completo; d) definir los requisitos para la expiración de los derechos de acceso privilegiado; e) establecer los derechos de acceso privilegiado a través de una identificación de usuario diferente de la usada para las actividades regulares del negocio. Las actividades regulares del negocio no se ejecutan desde una identificación privilegiada; f) tener las competencias de los usuarios con derechos de acceso privilegiado y su revisión periódica para verificar si están en línea con sus deberes; g) establecer y mantener procedimientos genéricos para evitar el uso no autorizado de identificaciones de usuario de administración genérica, de acuerdo con las capacidades de configuración del sistema; h) establecer la confidencialidad de la información de autenticación secreta, para las identificaciones de usuario de administración genérica, cuando se comparta (cambiar las contraseñas con frecuencia, y cuando un usuario privilegiado ha dejado el trabajo o cambia de trabajo, comunicarlas entre	20	
T.1.2.4	Responsable de SI	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	A.9.2.4		PR.AC-1	Revisar el proceso, que incluya: a) establecer la firma de una declaración para mantener confidencial la información de autenticación secreta personal, y mantener la información de autenticación secreta del grupo (cuando es compartida) únicamente dentro de los miembros del grupo; esta declaración firmada se puede incluir en los términos y condiciones del empleo para todos los que los usuarios ; b) estipular que todos los usuarios deben mantener su propia información de autenticación secreta, y se les suministra una autentificación secreta temporal segura, que se obligue a cambiar al usarla por primera vez; c) establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle la nueva información de autenticación secreta de reemplazo o temporal; d) definir que la información de autenticación secreta temporal se suministra a los usuarios de una manera segura; y se evitar utilizar partes externas o de mensajes de correo electrónico no protegidos (texto claro); e) establecer que la información de autenticación secreta temporal es única para un individuo y no es fácil de adivinar; f) definir que los usuarios deben acusar recibo de la información de autenticación secreta; g) establecer que la información de autenticación secreta por defecto, del fabricante, se modifica después de la instalación de los sistemas o software.	20	

T.1.2.5	Responsable de SI	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	A.9.2.5			Revisar los derechos de acceso que incluya: a) examinar los derechos de acceso de los usuarios periódicamente y después de cualquier cambio, promoción, cambio a un cargo a un nivel inferior, o terminación del empleo; b) establecer que los derechos de acceso de usuario se revisan y reasignan cuando pasan de un rol a otro dentro de la misma organización; c) definir las autorizaciones para los derechos de acceso privilegiado y revisar periódicamente; d) verificar las asignaciones de privilegios periódicamente, para asegurar que no se hayan obtenido privilegios no autorizados; e) revisar y registrar los cambios a las cuentas privilegiadas periódicamente.	20	
T.1.2.6	Responsable de SI	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	A.9.2.6			Revisar los derechos de acceso a la información y a los activos asociados con instalaciones de procesamiento de información, antes de que el empleo termine o cambie, dependiendo de la evaluación de factores de riesgo que incluya: a) terminación o cambio lo inicia el empleado, el usuario de la parte externa o la dirección, y la razón de la terminación; b) revisar las responsabilidades actuales del empleado, el usuario de la parte externa o cualquier otro usuario; c) verificar el valor de los activos accesibles en la actualidad.	60	
T.1.3	**Responsable de SI**	**RESPONSABILIDADES DE LOS USUARIOS**	**Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.**	**A.9.3**	Modelo de madurez definido			**100**	
T.1.3.1	Responsable de SI	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	A.9.3.1		PR.AC-1	Revisar si el proceso de notificación a usuarios incluye: a) Mantener la confidencialidad de la información de autenticación secreta, asegurándose de que no sea divulgada a ninguna otra parte, incluidas las personas con autoridad; b) evitar llevar un registro (en papel, en un archivo de software o en un dispositivo portátil) de autenticación secreta, a menos que se pueda almacenar en forma segura y que el método de almacenamiento haya sido aprobado (una bóveda para contraseñas); c) cambiar la información de autenticación secreta siempre que haya cualquier indicio de que se pueda comprometer la información; d) definir que cuando se usa contraseñas como información de autenticación secreta, se debe seleccionar contraseñas seguras con una longitud mínima suficiente que: 1) sean fáciles de recordar; 2) no estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.); 3) no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios); 4) estén libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos; 5) si son temporales, cambiarlos la primera vez que se ingrese; e) no compartir información de autenticación secreta del usuario individual; f) establecer una protección apropiada de contraseñas cuando se usan éstas como información de autenticación secreta en procedimientos de ingreso automatizados, y estén almacenadas; g) no usar la misma información de autenticación secreta para propósitos de negocio y otros diferentes de estos.	100	
T.1.4	Responsable de SI	**CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**	**Se debe evitar el acceso no autorizado a sistemas y aplicaciones.**	**A.9.4**	Modelo de madurez gestionado cuantitativamente			**52**	
T.1.4.1	Responsable de SI	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	A.9.4.1		PR.AC-4 PR.DS-5	Revisar las restricciones de acceso a través de la aplicación individual del negocio y de acuerdo con la política de control de acceso definida; que incluya: a) suministrar menús para controlar el acceso a las funciones de sistemas de aplicaciones; b) controlar a qué datos puede tener acceso un usuario particular; c) controlar los derechos de acceso de los usuarios, (a leer, escribir, borrar y ejecutar); d) controlar los derechos de acceso de otras aplicaciones; e) limitar la información contenida en los elementos de salida; f) proveer controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos.	20	

T.1.4.2	Responsable de SI	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	A.9.4.2		PR.AC-1	Revisar el procedimiento de ingreso que incluya: a) no visualizar los identificadores del sistema o de la aplicación sino hasta que el proceso de ingreso se haya completado exitosamente; b) visualizar una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador; c) evitar los mensajes de ayuda durante el procedimiento de ingreso, que ayudarían a un usuario no autorizado; d) validar la información de ingreso solamente al completar todos los datos de entrada. ante una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta; e) proteger contra intentos de ingreso mediante fuerza bruta; f) llevar un registro con los intentos exitosos y fallidos; g) declarar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de ingreso; h) visualizar la siguiente información al terminar un ingreso seguro: 1) registrar la fecha y la hora del ingreso previo exitoso; 2) registrar los detalles de cualquier intento de ingreso no exitoso desde el último ingreso exitoso; i) no visualizar una contraseña que se esté ingresando; j) no transmitir contraseñas en un texto claro en una red; k) terminar sesiones inactivas después de un período de inactividad definido, especialmente en lugares de alto riesgo tales como áreas públicas o externas por fuera de la gestión de seguridad de la organización o en dispositivos móviles; l) restringir los tiempos de conexión para brindar seguridad adicional para aplicaciones de alto riesgo y para reducir la ventana de oportunidad para acceso no autorizado.	60	
T.1.4.3	Responsable de TICs	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	A.9.4.3		PR.AC-1	Revisar el sistema de gestión de contraseñas que incluya: a) cumplir el uso de identificaciones y contraseñas de usuarios individuales para mantener la rendición de cuentas; b) permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluyan un procedimiento de confirmación para permitir los errores de entrada; c) Exigir por que se escojan contraseñas de calidad; d) Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez; e) Exigir por que se cambien las contraseñas en forma regular, según sea necesario: f) llevar un registro de las contraseñas usadas previamente, e impedir su reusó; g) no visualizar contraseñas en la pantalla cuando se está ingresando; h) almacenar los archivos de las contraseñas separadamente de los datos del sistema de aplicaciones; i) almacenar y transmitir las contraseñas en forma protegida.	100	
T.1.4.4	Responsable de TICs	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	A.9.4.4		PR.AC-4 PR.DS-5	Revisar las directrices para el uso de programas utilitarios con la capacidad de anular los controles de sistemas y de aplicaciones, que incluyan. a) utilizar procedimientos de identificación, autenticación y autorización para los programas utilitarios; b) separar los programas utilitarios del software de aplicaciones; c) limitar el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados; d) autorizar el uso adhoc de programas utilitarios; e) limitar la disponibilidad de los programas utilitarios; f) registrar el uso de los programas utilitarios; g) definir y documentar los niveles de autorización para los programas utilitarios; h) retirar o deshabilitar todos los programas utilitarios innecesarios; i) No poner a disposición los programas utilitarios a los usuarios que tengan acceso a aplicaciones en sistemas en donde se requiera la separación de deberes.	60	

T.1.4.5	Responsable de TICs	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	A.9.4.5		PR.DS-5	Revisar el procedimiento para la gestión de códigos fuente de los programas, que incluya: a) definir en donde sea posible, las librerías de fuentes de programas no se deben mantener en los sistemas operativos; b) gestionar los códigos fuente de los programas y las librerías de las fuentes de los programas se debería hacer de acuerdo con procedimientos establecidos; c) establecer que el personal de soporte deben tener acceso restringido a las librerías de las fuentes de los programas; d) definir que la actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores sólo se deben hacer una vez que se haya recibido autorización apropiada; e) establecer que los listados de programas se deben mantener en un entorno seguro; f) conservar un registro de auditoría de todos los accesos a la librerías de fuentes de programas; g) mantener y copiar las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios.	20	
CRIPTOGRAFÍA									
T.2	**Responsable de SI**	**CRIPTOGRAFÍA**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización** **Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles**	**A.10**				**100**	
T.2.1	**Responsable de SI**	**CONTROLES CRIPTOGRÁFICOS**	**Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.**	**A.10.1**	Modelo de madurez gestionado cuantitativamente			**100**	
T.2.1.1	Responsable de SI	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	A.10.1.1			Revisar la política sobre el uso de la criptográfica, que incluya: a) establecer el enfoque de la dirección con relación al uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se deben proteger la información del negocio; b) realizar una valoración de riesgos, que identifique el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido. c) utilizar la encriptación para la protección de información transportada por dispositivos de encriptación móviles o removibles, o a través de líneas de comunicación; d) gestionar las llaves y los métodos para la protección de llaves criptográficas y la recuperación de información encriptada, en el caso de llaves perdidas, llaves cuya seguridad está comprometida, o que están dañadas; e) establecer roles y responsabilidades, quién es responsable por: 1) la implementación de la política. 2) la gestión de llaves, incluida la generación de llaves; f) establecer las normas que se van a adoptar para la implementación efectiva en toda la organización (procesos del negocio); g) definir el impacto de usar información encriptada en los controles que dependen de la inspección del contenido.	100	
T.2.1.2	Responsable de SI	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	A.10.1.2			Revisar el sistema de gestión de llaves que debe estar basado en un grupo establecido de normas, procedimientos y métodos seguros para: a) generar llaves para diferentes sistemas criptográficos y diferentes aplicaciones; b) generar y obtener certificados de llaves públicas; c) distribuir llaves a las entidades previstas, incluyendo la forma de recibir y activar las llaves; d) almacenar las llaves, incluyendo la forma en que los usuarios autorizados obtienen acceso a ellas; e) cambiar o actualizar las llaves, incluyendo las reglas sobre cuándo se deben cambiar y cómo hacerlo; f) dar tratamiento a las llaves cuya seguridad está comprometida; g) revocar las llaves, incluyendo la forma de retirarlas o desactivarlas, cuando la seguridad de las llaves ha estado comprometida, o cuando un usuario deja la organización; h) recuperar las llaves que estén perdidas o dañadas; i) hacer copias de respaldo de las llaves o archivarlas; j) destruir las llaves; k) registrar y auditar las actividades relacionadas con gestión de llaves.	100	
SEGURIDAD FÍSICA Y DEL ENTORNO									

T.3	**Responsable de la seguridad física/Responsable de SI/Líderes de los procesos**	**SEGURIDAD FÍSICA Y DEL ENTORNO**		**A.11**				58	
T.3.1	**Responsable de la seguridad física**	**ÁREAS SEGURAS**	**Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.**	**A.11.1**	Modelo de madurez definido			**40**	
T.3.1.1	Responsable de la seguridad física	Perímetro de seguridad física	Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	A.11.1.1		PR.AC-2	Revisar las directrices relacionadas con los perímetros de seguridad física: a) definir los perímetros de seguridad, y el emplazamiento y fortaleza de cada uno de los perímetros deben depender de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de una valoración de riesgos; b) establecer los perímetros de una edificación o sitio que contenga instalaciones de procesamiento de la información debe ser físicamente seguros; el techo exterior, las paredes y el material de los pisos del sitio deben ser de construcción sólida, y todas las paredes externas deben estar protegidas adecuadamente contra acceso no autorizado con mecanismos de control (barras, alarmas, cerraduras); las puertas y ventanas deben estar cerradas con llave cuando no hay supervisión, y se debe considerar protección externa para ventanas, particularmente al nivel del suelo; c) definir un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación; el acceso a los sitios y edificaciones debe estar restringido únicamente para personal autorizado; d) establecer cuando sea aplicable y construir barreras físicas para impedir el acceso físico no autorizado y la contaminación ambiental; e) establecer que todas las puertas contra incendio en un perímetro de seguridad deben tener alarmas, estar monitoreadas y probadas junto con las paredes, para establecer el nivel requerido de resistencia de acuerdo con normas regionales, nacionales e internacionales adecuadas; deben funcionar de manera segura de acuerdo al código local de incendios; f) instalar sistemas adecuados para detección de intrusos de acuerdo con normas nacionales, regionales o internacionales y se deben probar regularmente para abarcar todas las puertas externas y ventanas accesibles; las áreas no ocupadas deben tener alarmas en todo momento; también deben abarcar otras áreas, tales como las salas de computo o las salas de	20	
T.3.1.2	Responsable de SI	Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	A.11.1.2		PR.AC-2 PR.MA-1	Revisar los controles de acceso físico y las siguientes directrices: a) tener un registro de la fecha y hora de entrada y salida de los visitantes, y todos los visitantes deben ser supervisados a menos que su acceso haya sido aprobado previamente; solo se les debe otorgar acceso para propósitos específicos autorizados y se deben emitir instrucciones sobre los requisitos de seguridad del área y de los propósitos de emergencia. La identidad de los visitantes se deben autenticar por los medios apropiados; b) establecer que el acceso a las áreas en las que se procesa o almacena información confidencial se debería restringir a los individuos autorizados solamente mediante la implementación de controles de acceso apropiados, (mediante la implementación de un mecanismo de autenticación de dos factores, tales como una tarjeta de acceso y un PIN secreto); c) mantener y hacer seguimiento de un libro de registro (physical log book) físico o un rastro de auditoría electrónica de todos los accesos; d) definir que todos los empleados, contratistas y partes externas deben portar algún tipo de identificación visible, y se deben notificar de inmediato al personal de seguridad si se encuentran visitantes no acompañados, y sin la identificación visible; e) establecer que el personal de servicio de soporte de la parte externa se le debería otorgar acceso restringido a áreas seguras o a instalaciones de procesamiento de información confidencial solo cuando se requiera; este acceso se deben autorizar y se le debe hacer seguimiento; f) definir los derechos de acceso a áreas seguras se deben revisar y actualizar regularmente, y revocar cuando sea necesario.	60	

T.3.1.3	Líderes de los procesos	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	A.11.1.3			Revisar las siguientes directrices relacionadas con la seguridad a oficinas, recintos e instalaciones: a) establecer que las instalaciones clave deben estar ubicadas de manera que se impida el acceso del público; b) definir donde sea aplicable, las edificaciones deben ser discretas y dar un indicio mínimo de su propósito, sin señales obvias externas o internas, que identifiquen la presencia de actividades de procesamiento de información; c) establecer que las instalaciones deben estar configuradas para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también se debe ser el apropiado; d) definir los directorios y guías telefónicas internas que identifican los lugares de las instalaciones de procesamiento de información confidencial no deben ser accesibles a ninguna persona no autorizada.	60	
T.3.1.4	Responsable de SI	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	A.11.1.4		ID.BE-5 PR.AC-2 PR.IP-5	De acuerdo a la NIST deben identificarse los elementos de resiliencia para soportar la entrega de los servicios críticos de la entidad.	20	
T.3.1.5	Responsable de SI	Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	A.11.1.5	Componente planeación		Revisar trabajo en área segura y las siguientes directrices: a) establecer que el personal solo debe conocer de la existencia de un área segura o de actividades dentro de un área segura, con base en lo que necesita conocer; b) definir que el trabajo no supervisado en áreas seguras se debe evitar tanto por razones de seguridad como para evitar oportunidades para actividades malintencionadas; c) establecer que las áreas seguras vacías deben estar cerradas con llave y se revisan periódicamente; d) no se permite el ingreso y uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.	40	
T.3.1.6	Responsable de la seguridad física	Áreas de despacho y carga	Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	A.11.1.6		PR.AC-2	Revisar las siguientes directrices: a) establecer que el acceso al área de despacho y de carga desde el exterior de la edificación se debería restringir al personal identificado y autorizado; b) definir que el área de despacho y carga se debe diseñar de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras partes de la edificación; c) establecer que las puertas externas de un área de despacho y carga se aseguran cuando las puertas internas están abiertas; d) definir que el material que ingresa se inspecciona y examina para determinar la presencia de explosivos, químicos u otros materiales peligrosos, antes de que se retiren del área de despacho y carga; e) establecer que el material que ingresa se registra de acuerdo con los procedimientos de gestión de activos al entrar al sitio; f) definir que los despachos entrantes y salientes se están separados físicamente, en donde sea posible; g) establecer que el material entrante se inspecciona para determinar evidencia de manipulación durante el viaje. Si se descubre esta manipulación, se debería reportar de inmediato al personal de seguridad.	n/a	
T.3.2	**Responsable de SI**	**EQUIPOS**	**Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.**	**A.11.2**	Modelo de madurez definido			**75**	

T.3.2.1	Responsable de SI	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	A.11.2.1		PR.IP-5	Revisar las siguientes directrices para proteger los equipos: a) establecer que los equipos están ubicados de manera que se minimice el acceso innecesario a las áreas de trabajo; b) definir que las instalaciones de procesamiento de la información que manejan datos sensibles están ubicadas cuidadosamente para reducir el riesgo de que personas no autorizadas puedan ver la información durante su uso; c) establecer que las instalaciones de almacenamiento se aseguran para evitar el acceso no autorizado; d) definir que los elementos que requieren protección especial se salvaguardan para reducir el nivel general de protección requerida; e) establecer los controles para minimizar el riesgo de amenazas físicas y ambientales, (robo, incendio, explosivos, humo, agua (o falla en el suministro de agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo); f) establecer directrices acerca de comer, consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información; g) hacer seguimiento de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente las instalaciones de procesamiento de información; h) proteger contra descargas eléctricas atmosféricas se debe aplicar a todas las edificaciones y se deben colocar filtros a todas las líneas de comunicaciones y de potencia entrantes, para la protección contra dichas descargas; i) considerar el uso de métodos de protección especial, tales como membranas para teclados, para equipos en ambientes industriales; j) proteger los equipos para procesamiento de información confidencial	60	
T.3.2.2	Responsable de TICs	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	A.11.2.2		ID.BE-4 PR.IP-5	Revisar los servicios de suministro (electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) para que cumplan: a) cumplir con las especificaciones de los fabricantes de equipos y con los requisitos legales locales; b) evaluar regularmente en cuanto a su capacidad para estar al ritmo del crecimiento e interacciones del negocio con otros servicios de soporte; c) inspeccionar y probar regularmente para asegurar su funcionamiento apropiado; d) si es necesario, contar con alarmas para detectar mal funcionamiento; e) si es necesario, tener múltiples alimentaciones con diverso enrutado físico.	100	
T.3.2.3	Responsable de TICs	Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información deben estar protegido contra interceptación, interferencia o daño.	A.11.2.3		ID.BE-4 PR.AC-2 PR.IP-5	Revisar las siguientes directrices para seguridad del cableado: a) establecer que las líneas de potencia y de telecomunicaciones que entran a instalaciones de procesamiento de información deben ser subterráneas en donde sea posible, o deben contar con una protección alternativa adecuada; b) establecer que los cables de potencia están separados de los cables de comunicaciones para evitar interferencia; c) definir para sistemas sensibles o críticos los controles adicionales que se deben considerar incluyen: 1) la instalación de conduit apantallado y recintos o cajas con llave en los puntos de inspección y de terminación; 2) el uso de blindaje electromagnético para proteger los cables; 3) el inicio de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se conectan a los cables	80	
T.3.2.4	Responsable de TICs	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	A.11.2.4		PR.MA-1 PR.MA-2	Revisar las siguientes directrices para mantenimiento de equipos: a) mantener los equipos de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor; b) establecer que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos; c) llevar registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo; d) implementar los controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si éste lo lleva a cabo el personal en el sitio o personal externo a la organización; en donde sea necesario, la información confidencial se debe borrar del equipo, o el personal de mantenimiento debería retirarse (cleared) lo suficientemente de la información; e) cumplir todos los requisitos de mantenimiento impuestos por las políticas de seguros; f) establecer que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.	80	

T.3.2.5	Responsable de TICs	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	A.11.2.5		PR.MA-1	Revisar las siguientes directrices para el retiro de activos: a) identificar a los empleados y usuarios de partes externas que tienen autoridad para permitir el retiro de activos del sitio; b) establecer los límites de tiempo para el retiro de activos y verificar que se cumplen las devoluciones; c) definir cuando sea necesario y apropiado, registrar los activos se retiran del sitio y cuando se hace su devolución; d) documentar la identidad, el rol y la filiación de cualquiera que maneje o use activos, y devolver esta documentación con el equipo, la información y el software. Información adicional	60	
T.3.2.6	Responsable de SI	Seguridad de equipos y activos fuera de las instalaciones	Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	A.11.2.6		ID.AM-4	De acuerdo a la NIST se deben catalogar los sistemas de información externos. Revisar las siguientes directrices para proteger los equipos fuera de las instalaciones: a) establecer que los equipos y medios retirados de las instalaciones no se deben dejar sin vigilancia en lugares públicos; b) seguir en todo momento las instrucciones del fabricante para proteger los equipos, (contra exposición a campos electromagnéticos fuertes); c) controlar los lugares fuera de las instalaciones, tales como trabajo en la casa, teletrabajo y sitios temporales se deben determinar mediante una valoración de riesgos y se deben aplicar los controles adecuados según sean apropiados, (gabinetes de archivo con llave, política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina); d) establecer que cuando el equipo que se encuentra afuera de las instalaciones es transferido entre diferentes individuos y partes externas, llevar un registro que defina la cadena de custodia para el equipo, que incluya al menos los nombres y las organizaciones de los responsables del equipo.	60	
T.3.2.7	Responsable de TICs	Disposición segura o reutilización de equipos	Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	A.11.2.7		PR.DS-3 PR.IP-6	Revisar las siguientes directrices del proceso de borrado de discos y de encriptación del disco (para evitar la divulgación de la información confidencial cuando se dispone del equipo o se le da un destino diferente, siempre y cuando): a) establecer que el proceso de encriptación sea suficientemente fuerte y abarque todo el disco (incluido el espacio perdido, archivos temporales de intercambio, etc.); b) definir que las llaves de encriptación sean lo suficientemente largas para resistir ataques de fuerza bruta; c) establecer que las llaves de encriptación se mantengan confidenciales.	n/a	
T.3.2.8	Responsable de SI	Equipos de usuario desatendidos	Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.	A.11.2.8			Revisar que el procedimiento equipos de usuarios desatendidos incluya: a) establecer que se cierren las sesiones activas cuando hayan terminado, a menos que se puedan asegurar mediante un mecanismo de bloqueo apropiado (un protector de pantalla protegido con contraseña); b) establecer que es obligatorio salir de las aplicaciones o servicios de red cuando ya no los necesiten; c) asegurar que los computadores o dispositivos móviles contra uso no autorizado mediante el bloqueo de teclas o un control equivalente (acceso con contraseña, cuando no están en uso).	100	
T.3.2.9	Responsable de SI	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	A.11.2.9		PR.PT-2	Revisar las siguientes directrices para escritorio limpio: a) establecer que la información sensible o crítica del negocio, (sobre papel o en un medio de almacenamiento electrónico), se guarda bajo llave (idealmente, en una caja fuerte o en un gabinete u otro mueble de seguridad) cuando no se requiera, especialmente cuando la oficina esté desocupada. b) definir un procedimiento para la gestión de equipos desatendidos; los computadores y terminales deben estar fuera del sistema y estar protegidos con un sistema de bloqueo de la pantalla y el teclado, controlado por una contraseña, token o mecanismo similar de autenticación de usuario, y deben estar protegidos por bloqueo de teclas u otros controles, cuando no están en uso; c) evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (escáneres, cámaras digitales); d) establecer que los medios que contienen información sensible o clasificada se deben retirar de las impresoras inmediatamente.	60	
SEGURIDAD DE LAS OPERACIONES									
T.4	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS OPERACIONES**		**A.12**				**34**	
T.4.1	**Responsable de TICs**	**PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**	**Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.**	**A.12.1**	Modelo de madurez definido			**30**	

T.4.1.1	**Responsable de TICs**	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.	A.12.1.1			Revisar los procedimientos de operación con instrucciones operacionales, que incluyen: a) instalar y configurar sistemas; b) establecer el procesamiento y manejo de información, tanto automático como manual; c) establecer la gestión de las copias de respaldo; d) definir los requisitos de programación, incluidas las interdependencias con otros sistemas, los tiempos de finalización del primer y último trabajos; e) establecer las instrucciones para manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución del trabajo, incluidas las restricciones sobre el uso de sistemas utilitarios; f) definir contactos de apoyo y de una instancia superior, incluidos los contactos de soporte externo, en el caso de dificultades operacionales o técnicas inesperadas; g) establecer las instrucciones sobre manejo de medios y elementos de salida, tales como el uso de papelería especial o la gestión de elementos de salida confidenciales, incluidos procedimientos para la disposición segura de elementos de salida de trabajos fallidos; h) definir los procedimientos de reinicio y recuperación del sistema para uso en el caso de falla del sistema; i) definir la gestión de la información de rastros de auditoria y de información del log del sistema; j) establecer los procedimientos de seguimiento.	20	
T.4.1.2	Responsable de TICs	Gestión de cambios	Se debe controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	A.12.1.2		PR.IP-1 PR.IP-3	Revisar los procedimientos de control de cambios, que incluyen: a) Identificar y registrar los cambios significativos; b) Planificar y puesta a prueba de los cambios; c) Valorar los impactos potenciales, incluidos los impactos de estos cambios en la seguridad de la información; d) Tener un procedimiento de aprobación formal para los cambios propuestos; e) Verificar que se han cumplido los requisitos de seguridad de la información; f) Comunicar todos los detalles de los cambios a todas las personas pertinentes; g) Tener un procedimiento de apoyo, incluidos procedimientos y responsabilidades para abortar cambios no exitosos y recuperarse de ellos, y eventos no previstos; h) Contar con un suministro de un proceso de cambio de emergencia que posibilite la implementación rápida y controlada de los cambios necesarios para resolver un incidente.	20	
T.4.1.3	Responsable de TICs	Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	A.12.1.3		ID.BE-4	Revisar los procedimientos para la gestión de la demanda de capacidad, que incluyen: a) Eliminar datos obsoletos (espacio en disco); b) realizar cierre definitivo de aplicaciones, sistemas, bases de datos o ambientes; c) optimizar cronogramas y procesos de lotes; d) optimizar las consultas de bases de datos o lógicas de las aplicaciones; e) realizar una negación o restricción de ancho de banda a servicios ávidos de recursos, si estos no son críticos para el negocio (por ejemplo, video en tiempo real).	60	
T.4.1.4	Responsable de TICs	Separación de los ambientes de desarrollo, pruebas y operación	Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	A.12.1.4		PR.DS-7	Revisar los procedimientos para la separación de ambientes, que incluyen: a) definir y documentar las reglas para la transferencia de software del estatus de desarrollo al de operaciones. b) establecer que el software de desarrollo y de operaciones debe funcionar en diferentes sistemas o procesadores de computador y en diferentes dominios o directorios; c) definir que los cambios en los sistemas operativos y aplicaciones se deben probar en un entorno de pruebas antes de aplicarlos a los sistemas operacionales; d) definir que solo en circunstancias excepcionales, las pruebas no se deben llevar a cabo en los sistemas operacionales; e) establecer que los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no debe ser accesibles desde sistemas operacionales cuando no se requiere; f) establecer que los usuarios deben usar diferentes perfiles de usuario para sistemas operacionales y de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error; g) definir que los datos sensibles no se debe copiar en el ambiente del sistema de pruebas, a menos que se suministren controles equivalentes para el sistema de pruebas	20	

T.4.2	**Responsable de SI**	**PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS**	**Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.**	**A.12.2**				**20**	
T.4.2.1	**Responsable de SI**	Controles contra códigos maliciosos	Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	A.12.2.1	Modelo de madurez gestionado	PR.DS-6 DE.CM-4 RS.MI-2	Revisar las siguientes directrices: a) establecer una política formal que prohíba el uso de software no autorizado; b) implementar controles para evitar o detectar el uso de software no autorizado (listas blancas de aplicaciones); b) implementar controles para evitar o detectar el uso de sitios web malicioso o que se sospecha que lo son (listas negras); d) establecer una política formal para proteger contra riesgos asociados con la obtención de archivos y de software ya sea mediante redes externas o cualquier otro medio, indicando qué medidas externas se deben tomar; e) reducir las vulnerabilidades de las que pueda aprovecharse el software malicioso, (medio de la gestión de la vulnerabilidad técnica); f) llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos del negocio; se debería investigar formalmente la presencia de archivos no aprobados o de enmiendas no autorizadas; g) instalar y actualizar software de detección y reparación del software malicioso en los computadores y medios como una medida de control, en forma rutinaria; el análisis realizado debería incluir: 1) el análisis de cualquier archivo recibido por la red o por cualquier forma de medio de almacenamiento, para detectar el software malicioso, antes de uso; 2) el análisis de los adjuntos y descargas de los correos electrónicos, para determinación del software malicioso antes de uso; este análisis se debería llevar a cabo en diferentes lugares, (los servidores de los correos electrónicos, en los computadores de escritorio) y cuando se ingresa a la red de la organización; el análisis de páginas web, para determinar el software malicioso;	20	
T.4.3	**Responsable de TICs**	**COPIAS DE RESPALDO**	**Proteger contra la pérdida de datos.**	**A.12.3**	Modelo de madurez gestionado			**40**	
T.4.3.1	Responsable de TICs	Respaldo de la información	Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	A.12.3.1		PR.DS-4 PR.IP-4	Revisar las siguientes directrices: a) producir registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados; b) establecer la cobertura (copias de respaldo completas o diferenciales) y la frecuencia con que se hagan las copias de respaldo debe reflejar los requisitos del negocio de la organización, los requisitos de la seguridad de la información involucrada, y la criticidad de la información para la operación continua de la organización; c) definir las copias de respaldo se debe almacenar en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal; d) establecer la información de respaldo y un nivel apropiado de protección física y del entorno, de coherencia con las normas aplicadas en el sitio principal; e) definir los medios de respaldo se debe poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso necesario; esto se debería combinar con una prueba de los procedimientos de restauración, y se debe verificar contra el tiempo de restauración requerido. f) definir las situaciones en las que la confidencialidad tiene importancia, las copias de respaldo deben estar protegidas por medio de encriptación.	40	
T.4.4	Responsable de SI	**REGISTRO Y SEGUIMIENTO**	**Registrar eventos y generar evidencia.**	**A.12.4**	Modelo de madurez gestionado cuantitativamente			**25**	

T.4.4.1	Responsable de SI	Registro de eventos	Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	A.12.4.1	Modelo de madurez gestionado cuantitativamente	PR.PT-1 DE.CM-3 RS.AN-1	Revisar los registros de eventos que incluyan: a) identificar los usuarios; b) establecer las actividades del sistema; c) definir las fechas, horas y detalles de los eventos clave, (entrada y salida); d) identificar el dispositivo o ubicación, si es posible, e identificador del sistema; e) tener registros de intentos de acceso al sistema exitosos y rechazados; e) definir registros de datos exitosos y rechazados y otros intentos de acceso a recursos; g) establecer los cambios a la configuración del sistema; h) definir el uso de privilegios; i) establecer el uso de utilitarios y aplicaciones del sistema; j) definir los archivos a los que se tuvo acceso, y el tipo de acceso; k) establecer las direcciones y protocolos de red; l) definir las alarmas accionadas por el sistema de control de acceso; m) activar y desactivar los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión; n) registrar las transacciones ejecutadas por los usuarios en las aplicaciones.	20	
T.4.4.2	Responsable de SI	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	A.12.4.2		PR.PT-1	Revisar los procedimientos y controles dirigidos a proteger contra cambios no autorizados de la información del registro y contra problemas con la instalación de registro, que incluya: a) verificar todas las alteraciones a los tipos de mensaje que se registran; b) establecer los archivos log que son editados o eliminados; c) verificar cuando se excede la capacidad de almacenamiento del medio de archivo log, lo que da como resultado falla en el registro de eventos, o sobre escritura de eventos pasados registrados.	20	
T.4.4.3	Responsable de SI	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se debe registrar, y los registros se deben proteger y revisar con regularidad.	A.12.4.3		PR.PT-1 RS.AN-1	Revisar los registros de las actividades del administrador y del operador del sistema, los registros se deben proteger y revisar con regularidad.	40	
T.4.4.4	Responsable de SI	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	A.12.4.4		PR.PT-1	Revisar se deberían sincronizar con una única fuente de referencia de tiempo Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.	20	
T.4.5	**Responsable de TICs**	**CONTROL DE SOFTWARE OPERACIONAL**	**Asegurar la integridad de los sistemas operacionales.**	**A.12.5**	Modelo de madurez definido			**60**	
T.4.5.1	Responsable de TICs	Instalación de software en sistemas operativos	Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.	A.12.5.1		PR.DS-6 PR.IP-1 PR.IP-3 DE.CM-5	Revisar las siguientes directrices para control de software operacional: a) actualizar el software operacional, aplicaciones y bibliotecas de programas solo la debe llevar a cabo administradores entrenados, con autorización apropiada de la dirección; b) definir que los sistemas operacionales sólo debe contener códigos ejecutables aprobados, no el código de desarrollo o compiladores; c) establecer que las aplicaciones y el software del sistema operativo solo se debe implementar después de pruebas extensas y exitosas; los ensayos deben abarcar la usabilidad, la seguridad, los efectos sobre otros sistemas y la facilidad de uso, y se debe llevar a cabo en sistemas separados; se debe asegurar que todas las bibliotecas de fuentes de programas correspondientes hayan sido actualizadas; d) usar un sistema de control de la configuración para mantener el control de todo el software implementado, al igual que la documentación del sistema; e) establecer una estrategia de retroceso (rollback) antes de implementar los cambios; f) mantener un log de auditoría de todas las actualizaciones de las bibliotecas de programas operacionales; g) definir las versiones anteriores del software de aplicación se deben conservar como una medida de contingencia; h) establecer que las versiones de software anteriores se deben llevar al archivo permanente, junto con toda la información y parámetros, procedimientos, detalles de configuración y software de soporte anteriores, en tanto los datos permanezcan en el archivo permanente.	60	
T.4.6	**Responsable de SI**	**GESTIÓN DE LA VULNERABILIDAD TÉCNICA**	**Prevenir el aprovechamiento de las vulnerabilidades técnicas.**	**A.12.6**	Modelo de madurez gestionado			**40**	

T.4.6.1	Responsable de SI	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	A.12.6.1		ID.RA-1 ID.RA-5 PR.IP-12 DE.CM-8 RS.MI-3	Revisar las siguientes directrices para vulnerabilidades técnicas: a) definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida; b) definir los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellos se debe identificar para el software y otra tecnología; c) una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes potencialmente; d) establecer que una vez que se haya identificado una vulnerabilidad técnica potencial, la organización debería identificar los riesgos asociados y las acciones por tomar; esta acción puede involucrar la colocación de parches de sistemas vulnerables o la aplicación de otros controles; Si no es posible colocar controles se deben documentar en los riesgos de acuerdo a su probabilidad e impacto y colocarlo como riesgo aceptado. e) definir dependiendo de la urgencia con la que se necesite tratar una vulnerabilidad técnica, la acción tomada se debería llevar a cabo de acuerdo con los controles relacionados con la gestión de cambios, o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información; f) establecer, si está disponible un parche de una fuente legítima, se debe valorar los riesgos asociados con la instalación del parche (los riesgos que acarrea la vulnerabilidad se debe comparar con el riesgo de instalar el parche); g) establecer que los parches se deben probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos	60	
T.4.6.2	Responsable de TICs	Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	A.12.6.2		PR.IP-1 PR.IP-3	Revisar las restricciones y las reglas para la instalación de software por parte de los usuarios.	20	
T.4.7	**Responsable de TICs**	**CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN**	**Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.**	**A.12.7**	Modelo de madurez gestionado cuantitativamente			**20**	
T.4.7.1	Responsable de TICs	Controles sobre auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se debe planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	A.12.7.1			Revisar las siguientes directrices para las auditorias de sistemas de información: a) establecer los requisitos de auditoría para acceso a sistemas y a datos se debe acordar con la dirección apropiada; b) definir el alcance de las pruebas técnicas de auditoría se debe acordar y controlar; c) establecer las pruebas de auditoría se debe limitar a acceso a software y datos únicamente para lectura; d) definir el acceso diferente al de solo lectura solamente se debe prever para copias aisladas de los archivos del sistema, que se deben borrar una vez que la auditoría haya finalizado, o se debe proporcionar información apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría; e) definir los requisitos para procesos especiales y adicionales se debe identificar y acordar; f) establecer las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales; g) hacer seguimiento de todos los accesos y logged para producir un rastro de referencia.	20	
SEGURIDAD DE LAS COMUNICACIONES									
T.5	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS COMUNICACIONES**		**A.13**				33	
T.5.1	**Responsable de TICs**	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**	**Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.**	**A.13.1**	Modelo de madurez definido			**40**	

T.5.1.1	Responsable de TICs	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1		PR.AC-3 PR.AC-5 PR.DS-2 PR.PT-4	Revisar las siguientes directrices para la gestión de seguridad de redes: a) establecer las responsabilidades y procedimientos para la gestión de equipos de redes; b) definir la responsabilidad operacional por las redes se debería separar de las operaciones informáticas, en donde sea apropiado; c) establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre redes inalámbricas, y para proteger los sistemas y aplicaciones conectados; d) De acuerdo a NIST, Gestionar el acceso remoto d) aplicar logging y seguimiento adecuados para posibilitar el registro y detección de acciones que pueden afectar, o son pertinentes a la seguridad de la información; e) definir las actividades de gestión a coordinar estrechamente tanto para optimizar el servicio de la organización, como para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información; f) establecer los sistemas en la red que se autenticar; g) restringir la conexión de los sistemas a la red.	20	
T.5.1.2	Responsable de SI	Seguridad de los servicios de red	Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	A.13.1.2			Revisar las siguientes directrices para la seguridad de los servicios de red: a) establecer la tecnología aplicada a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red; b) definir los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red; c) establecer los procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.	60	
T.5.1.3	Responsable de TICs	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	A.13.1.3		PR.AC-5 PR.DS-5	De acuerdo a NIST se debe proteger la integridad de las redes incorporando segregación donde se requiera.	40	
T.5.2	**Responsable de TICs**	**TRANSFERENCIA DE INFORMACIÓN**	**Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.**	**A.13.2**	Modelo de madurez definido			**25**	
T.5.2.1	Responsable de TICs	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	A.13.2.1		ID.AM-3 PR.AC-5 PR.AC-3 PR.DS-2 PR.DS-5 PR.PT-4	De acuerdo a la NIST: Se deben mapear los flujos de comunicaciones y datos para poder cumplir con este ítem. Revisar las siguientes directrices: a) definir los procedimientos diseñados para proteger la información transferida contra interceptación, copiado, modificación, enrutado y destrucción; b) definir los procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas; c) definir los procedimientos para proteger información electrónica sensible comunicada que están como adjuntos; d) establecer la política o directrices que presentan el uso aceptable de las instalaciones de comunicación; e) definir las responsabilidades del personal, las partes externas y cualquier otro usuario no comprometen a la organización, (por difamación, acoso, suplantación, envío de cadenas, compras no autorizadas, etc.); f) establecer el uso de técnicas criptográficas, (proteger la confidencialidad, la integridad y la autenticidad de la información). g) establecer las directrices sobre retención y disposición para toda la correspondencia del negocio, incluidos mensajes, de acuerdo con la legislación y reglamentaciones locales y nacionales; h) definir los controles y restricciones asociadas con las instalaciones de comunicación, (el reenvío automático de correo electrónico a direcciones de correo externas); i) brindar asesoría al personal para que tome las precauciones apropiadas acerca de no revelar información confidencial; j) no dejar mensajes que contengan información confidencial, en las máquinas contestadoras, ya que éstos pueden ser escuchados por personas	20	

T.5.2.2	Responsable de TICs	Acuerdos sobre transferencia de información	Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	A.13.2.2			Revisar las siguientes directrices para transferencia segura de la información: a) establecer las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo; b) definir los procedimientos para asegurar trazabilidad y no repudio; c) definir los estándares técnicos mínimos para empaquetado y transmisión; d) tener certificados de depósito de títulos en garantía; e) establecer los estándares de identificación de mensajería; f) definir las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos; g) establecer el uso de un sistema de etiquetado acordado para información sensible o crítica, que asegure que el significado de la etiqueta se entiende de inmediato, y que la información está protegida apropiadamente; h) definir las normas técnicas para registro y lectura de información y software; i) cualquier control especial que se requiera para proteger elementos críticos, tales como criptografía; j) mantener una cadena de custodia para la información mientras está en tránsito; k) definir los niveles aceptables de control de acceso.	20	
T.5.2.3	Responsable de TICs	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	A.13.2.3		PR.DS-2 PR.DS-5	Revisar las siguientes directrices para mensajería electrónica: a) definir la protección de mensajes contra acceso no autorizado, modificación o denegación del servicio proporcionales al esquema de clasificación adoptado por la organización; b) asegurar el direccionamiento y transporte correctos del mensaje; c) establecer la confiabilidad y disponibilidad del servicio; d) definir las consideraciones legales, (los requisitos para firmas electrónicas; e) establecer la obtención de aprobación antes de usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información); f) definir niveles más fuertes de autenticación para control del acceso desde redes accesibles públicamente.	40	
T.5.2.4	Responsable de SI	Acuerdos de confidencialidad o de no divulgación	Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	A.13.2.4		PR.DS-5	Revisar las siguientes directrices para acuerdos de confidencialidad: a) definir la información que se va a proteger (información confidencial); b) determinar la duración esperada de un acuerdo, incluidos los casos en los que podría ser necesario mantener la confidencialidad indefinidamente; c) establecer las acciones requeridas cuando termina el acuerdo; d) definir las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información; e) definir la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de información confidencial; f) definir el uso permitido de información confidencial y los derechos del firmante para usar la información; g) establecer el derecho a actividades de auditoría y de seguimiento que involucran información confidencial; h) definir el proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial; i) definir los plazos para que la información sea devuelta o destruida al cesar el acuerdo; j) establecer las acciones que se espera tomar en caso de violación del acuerdo.	20	
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS									
T.6	**Responsable de SI/Responsable de TICs**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		**A.14**				36	
T.6.1	**Responsable de SI**	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**	**Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.**	**A.14.1**	Modelo de madurez definido			**40**	

T.6.1.1	Responsable de SI	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se debe incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	A.14.1.1		PR.IP-2	Revisar las siguientes directrices para análisis y especificaciones de requisitos de seguridad de la información: a) establecer el nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario. b) definir los procesos de suministro de acceso y de autorización para usuarios del negocio, al igual que para usuarios privilegiados o técnicos; c) informar a los usuarios y operadores sobre sus deberes y responsabilidades; d) definir las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad, integridad; e) definir los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso y seguimiento, y de no repudio; f) establecer los requisitos exigidos por otros controles de seguridad, (interfaces con el ingreso o seguimiento, o los sistemas de detección de fuga de datos).	40	
T.6.1.2	Responsable de SI	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2		PR.DS-2 PR.DS-5 PR.DS-6	Revisar las siguientes directrices para la seguridad de servicios de las aplicaciones en redes públicas: a) definir el nivel de confianza que cada parte requiere con relación a la identidad declarada por la otra parte, (por medio de autenticación); b) establecer los procesos de autorización asociados con quien puede aprobar el contenido o expedir o firmar documentos transaccionales clave; c) asegurar que los socios de comunicación estén completamente informados de sus autorizaciones para suministro o uso del servicio; d) determinar y cumplir los requisitos para confidencialidad, integridad, prueba de despacho y recibo de documentos clave y el no repudio de los contratos, (asociados con procesos de ofertas y contratos); e) definir el nivel de confianza requerido en la integridad de los documentos clave; f) establecer los requisitos de protección de cualquier información confidencial; g) definir la confidencialidad e integridad de cualquier transacción de pedidos, información de pagos, detalles de la dirección de entrega y confirmación de recibos; h) definir el grado de verificación apropiado de la información de pago suministrada por un cliente; i) seleccionar la forma de arreglo de pago más apropiado para protegerse contra fraude; j) definir el nivel de protección requerido para mantener la confidencialidad e integridad de la información del pedido; k) evitar la pérdida o duplicación de información de la transacción; l) definir la responsabilidad civil asociada con cualquier transacción fraudulenta;	40	
T.6.1.3	Responsable de SI	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	A.14.1.3		PR.DS-2 PR.DS-5 PR.DS-6	Revisar las siguientes directrices protección de transacciones de los servicios de las aplicaciones: a) definir el uso de firmas electrónicas por cada una de las partes involucradas en la transacción; b) establecer todos los aspectos de la transacción, es decir, asegurar que: 1) definir la información de autenticación secreta de usuario, de todas las partes, se valide y verifique; 2) definir a transacción permanezca confidencial; 3) mantener la privacidad asociada con todas las partes involucradas; c) definir la trayectoria de las comunicaciones entre todas las partes involucradas esté encriptada; d) definir los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados; e) asegurar que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente, (en una plataforma de almacenamiento existente en la intranet de la organización, y no retenido ni expuesto en un medio de almacenamiento accesible directamente desde Internet); f) utilizar una autoridad confiable (para los propósitos de emitir y mantener firmas digitales o certificados digitales), la seguridad está integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.	20	
T.6.2	**Responsable de SI**	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE**	**Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.**	**A.14.2**	Modelo de madurez definido			**27**	

T.6.2.1	Responsable de SI	Política de desarrollo seguro	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	A.14.2.1		PR.IP-2	Revisar las siguientes directrices política de desarrollo seguro: a) definir la seguridad del ambiente de desarrollo; b) orientar la seguridad en el ciclo de vida de desarrollo del software: 1) definir la seguridad en la metodología de desarrollo de software; 2) establecer las directrices de codificación seguras para cada lenguaje de programación usado; c) definir los requisitos de seguridad en la fase diseño; d) definir los puntos de chequeo de seguridad dentro de los hitos del proyecto; e) establecer los depósitos seguros; f) definir la seguridad en el control de la versión; g) establecer el conocimiento requerido sobre seguridad de la aplicación; h) definir la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.	20	
T.6.2.2	Responsable de TICs	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se debe controlar mediante el uso de procedimientos formales de control de cambios.	A.14.2.2		PR.IP-1 PR.IP-3	Revisar las siguientes directrices procedimientos control de cambio en sistemas: a) llevar un registro de los niveles de autorización acordados; b) asegurar que los cambios se presenten a los usuarios autorizados; c) revisar los controles y procedimientos de integridad para asegurar que no se vean comprometidos por los cambios; d) identificar todo el software, información, entidades de bases de datos y hardware que requieren corrección; e) identificar y verificar el código crítico de seguridad para minimizar la posibilidad de debilidades de seguridad conocidas; f) obtener aprobación formal para propuestas detalladas antes de que el trabajo comience; g) revisar antes de la implementación, asegurar que los usuarios autorizados aceptan los cambios; h) asegurar que el conjunto de documentación del sistema está actualizado al completar cada cambio, y que la documentación antigua se lleva al archivo permanente, o se dispone de ella; i) mantener un control de versiones para todas las actualizaciones de software; j) mantener un rastro de auditoría de todas las solicitudes de cambio; k) asegurar que la documentación de operación y los procedimientos de los usuarios experimenten los cambios que les permitan seguir siendo apropiados; l) asegurar que la implementación de los cambios ocurre en el momento correcto y no afecta los procesos de negocio involucrados.	40	
T.6.2.3	Responsable de TICs	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	A.14.2.3		PR.IP-1	Revisar las siguientes directrices revisión técnica de las aplicaciones después de cambios en la plataforma de operación: a) revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones; b) asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación; c) asegurar que se hacen cambios apropiados en los planes de continuidad del negocio.	20	
T.6.2.4	Responsable de TICs	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	A.14.2.4		PR.IP-1	Revisar las siguientes directrices restricciones en los cambios a los paquetes de software: a) definir el riesgo de que los procesos de integridad y los controles incluidos se vean comprometidos; b) obtener el consentimiento del vendedor; c) obtener del vendedor los cambios requeridos, a medida que se actualiza el programa estándar; d) evaluar el impacto, si la organización llega a ser responsable del mantenimiento futuro del software como resultado de los cambios; e) definir la compatibilidad con otro software en uso.	20	
T.6.2.5	Responsable de TICs	Principios de construcción de sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	A.14.2.5		PR.IP-2	Revisar la documentación y los principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	20	

T.6.2.6	Responsable de TICs	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	A.14.2.6			Revisar las siguientes directrices para ambiente de desarrollo seguro: a) carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir; b) definir los requisitos externos e internos aplicables, (reglamentaciones o políticas); c) definir los controles de seguridad ya implementados por la organización, que brindan soportar al desarrollo del sistema; d) establecer la confiabilidad del personal que trabaja en el ambiente; e) definir el grado de contratación externa asociado con el desarrollo del sistema; f) definir la necesidad de separación entre diferentes ambientes de desarrollo; g) definir el control de acceso al ambiente de desarrollo; h) establecer el seguimiento de los cambios en el ambiente y en los códigos almacenados ahí; i) definir las copias de respaldo se almacenan en lugares seguros fuera del sitio; j) definir el control sobre el movimiento de datos desde y hacia el ambiente.	40	
T.6.2.7	Responsable de TICs	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	A.14.2.7		DE.CM-6	Revisar las siguientes directrices desarrollo contratado externamente: a) definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente; b) establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas; c) definir el suministro del modelo de amenaza aprobado, al desarrollador externo; d) realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables; e) definir la evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad; f) definir la evidencia de que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega; g) definir la evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas; h) definir los certificados de depósito de títulos en garantía; (el código fuente ya no está disponible); i) establecer el derecho contractual con relación a procesos y controles de desarrollo de auditorías; j) documentar eficaz del ambiente de construcción usado para crear entregables; k) establecer que la organización es responsable de la conformidad con las leyes aplicables y con la verificación de la eficiencia del control.	40	
T.6.2.8	Responsable de SI	Pruebas de seguridad de sistemas	Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.	A.14.2.8	Modelo de madurez gestionado cuantitativamente	DE.DP-3	Verifique en una muestra que para pasar a producción los desarrollos se realizan pruebas de seguridad. También verifique que los procesos de detección de incidentes son probados periódicamente.	20	
T.6.2.9	Responsable de TICs	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados.	A.14.2.9			Revisar las pruebas de aceptación de sistemas, para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.	20	
T.6.3	Responsable de SI	**DATOS DE PRUEBA**	**Asegurar la protección de los datos usados para pruebas.**	**A.14.3**	Modelo de madurez definido			**40**	
T.6.3.1	Responsable de SI	Protección de datos de prueba	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	A.14.3.1			Revisar las siguientes directrices para protección de datos de prueba: a) establecer los procedimientos de control de acceso, que se aplican a los sistemas de aplicación operacionales, se debe aplicar también a los sistemas de aplicación de pruebas; b) tener una autorización separada cada vez que se copia información operacional a un ambiente de pruebas; c) definir que la información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas; d) establecer que el copiado y uso de la información operacional se debe logged para suministrar un rastro de auditoría.	40	
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN									
T.7.	**Responsable de SI/Responsable de TICs**	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		**A.16**				20	

T.7.1	**Responsable de SI**	**GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**	**Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.**	**A.16.1**				**20**	
T.7.1.1	Responsable de SI	Responsabilidades y procedimientos	Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	A.16.1.1		PR.IP-9 DE.AE-2 RS.CO-1	Revisar las siguientes directrices responsabilidades y procedimientos: a) establecer las responsabilidades de gestión, para asegurar que los siguientes procedimientos se desarrollan y comunican adecuadamente dentro de la organización: 1) los procedimientos para la planificación y preparación de respuesta a incidentes; 2) los procedimientos para seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información; 3) los procedimientos para logging las actividades de gestión de incidentes; 4) los procedimientos para el manejo de evidencia forense; 5) los procedimientos para la valoración y toma de decisiones sobre eventos de seguridad de la información y la valoración de debilidades de seguridad de la información; 6) los procedimientos para respuesta, incluyendo aquellos para llevar el asunto a una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas; b) establecer los procedimientos para asegurar que: 1) el personal competente maneje las cuestiones relacionadas con incidentes de seguridad de la información dentro de la organización; 2) se implemente un punto de contacto para la detección y reporte de incidentes de seguridad; 3) se mantengan contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información; c) definir el reporte de procedimientos debería incluir: 1) la preparación de formatos de reporte de eventos de seguridad de la información para apoyar la acción de reporte y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento de	20	
T.7.1.2	Responsable de SI	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se debe informar a través de los canales de gestión apropiados, tan pronto como sea posible.	A.16.1.2	Modelo de madurez definido	DE.DP-4	Revisar las siguientes directrices reporte de eventos de seguridad de la información: a) establecer un control de seguridad ineficaz; b) definir la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información; c) definir los errores humanos; d) definir las no conformidades con políticas o directrices; e) definir las violaciones de acuerdos de seguridad física; f) establecer los cambios no controlados en el sistema; g) definir mal funcionamiento en el software o hardware; h) definir violaciones de acceso. **Tenga en cuenta para la calificación:** 1) Si se elaboran informes de TODOS los incidentes de seguridad y privacidad de la información, TODOS están documentados e incluidos en el plan de mejoramiento continuo. Se definen los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro, están en 40. 2) Si los controles y medidas identificados para disminuir los incidentes fueron implementados, están en 60.	20	
T.7.1.3	Responsable de SI	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	A.16.1.3	Modelo de madurez definido	RS.CO-2	Observe si los eventos son reportados de forma consistente en toda la entidad de acuerdo a los criterios establecidos.	20	
T.7.1.4	Responsable de SI	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se debe evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	A.16.1.4	Madurez Inicial	DE.AE-2 RS.AN-4	Revise si los eventos de SI detectados son analizados para determinar si constituyen un incidentes de seguridad de la información y entender los objetivos del ataque y sus métodos. Evidencia si los incidentes son categorizados y se cuenta con planes de respuesta para cada categoría.	20	

T.7.1.5	Responsable de SI	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	A.16.1.5	Modelo de madurez gestionado cuantitativamente	RS.RP-1 RS.AN-1 RS.MI-2 RC.RP-1 RC.RP-1	Revisar las siguientes directrices para respuesta a incidentes de seguridad de la información: a) Los incidentes son contenidos y la probabilidad de que vuelvan a ocurrir mitigada. b) Se debe contar con un plan de recuperación de incidentes durante o después del mismo. b) recolectar evidencia lo más pronto posible después de que ocurra el incidente; c) llevar a cabo análisis forense de seguridad de la información, según se requiera d) llevar el asunto a una instancia superior, según se requiera; e) asegurar que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior; f) comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo; g) tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente; g) establecer que una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto. h) de acuerdo a la NIST se deben investigar las notificaciones de los sistemas de detección. **Tenga en cuenta para la calificación:** 1) Si los planes de respuesta a incidentes incluyen algunas áreas de la entidad y si se evalúa la efectividad los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro es 60 2) Se incluyen todas las áreas de la Entidad, en los planes de respuesta de	20	
T.7.1.6	Responsable de TICs	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	A.16.1.6	Modelo de madurez gestionado cuantitativamente	DE.DP-5 RS.AN-2 RS.IM-1	De acuerdo a la NIST se debe entender cual fue el impacto del incidente. Las lecciones aprendidas deben ser usadas para actualizar los planes de respuesta a los incidentes de SI. **Tenga en cuenta para la calificación:** La Entidad aprende continuamente sobre los incidentes de seguridad presentados.	20	
T.7.1.7	Responsable de TICs	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	A.16.1.7	Modelo de madurez gestionado Modelo de madurez definido	RS.AN-3	Revisar las siguientes directrices para recolección de evidencia: a) definir la cadena de custodia; b) establecer la seguridad de la evidencia; c) definir la seguridad del personal; d) definir los roles y responsabilidades del personal involucrado; e) establecer la competencia del personal; f) realizar la documentación; g) definir las sesiones informativas.	20	