Elaborado por:	**Validado por:**	**Aprobado por:**
Laureano Esau Villamil Laitón		**Comité de Gestión y Desempeño**

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN PESI

INTRODUCCIÓN

La seguridad de la información, según ISO/IEC 27001:2013, consiste en preservar la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de un proceso de Gestión de Riesgo, (ISO/ IEC 27001 VERSION 2013, 2013), para lo cual, el proyecto busca dar respuesta a las exigencias que el Ministerio de Tecnologías de la Información y las comunicaciones de Colombia, (MinTic), presenta para todas entidades públicas.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse a los siguientes componentes:

TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

TIC para Gobierno Abierto que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

Este documento indica, definiendo plazos anuales, cuáles serán las labores que realizará Salud Sogamoso con el objetivo de lograr el 100% de la implementación del MSPI al interior de todos los procesos de la entidad.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización. Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

Las actividades para la administración y la seguridad informática pueden clasificarse en varias categorías como son: seguridad funcional, coordinación, documentación, certificación, acreditación, administración de configuraciones de sistemas y de seguridad informática y manejo de riesgos.

Este documento se elabora con el objetivo de orientar a la Entidad para dar cumplimiento con lo solicitado en el Decreto 612 de 2018 y todas las consideraciones expuestas, dentro de las cuáles se encuentra el decreto 1078 de 2015 y los instrumentos para implementar la Estrategia de Gobierno Digital, dentro de los cuales se exige la elaboración por parte de cada entidad, de un Plan de Seguridad y Privacidad de la Información.

En el presente documento se adoptó la concepción, metodología, lineamientos e instrumentos desarrollados por el Ministerio de Tecnologías de la Información y las Comunicaciones –MinTIC-, que conforman la Estrategia de Gobierno Digital, la cual está soportada en los LINEAMIENTOS PARA LA ELABORACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN (PESI) 1 y el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN2.

1. OBJETIVO PESI

Liderar y establecer las estrategias para la gestión de seguridad y privacidad de la Información en Salud Sogamoso E.S.E. que permitan minimizar los riesgos de pérdida de activos de la información y estén alineadas a la estrategia y modelo integrado de gestión y acordes con las necesidades de la Entidad y los lineamientos del programa de Gobierno Digital.

1.1. Objetivos específicos

El PESI de Salud Sogamoso E.S.E.- cuenta con los siguientes objetivos específicos acordes con las necesidades de la Entidad y las dimensiones de Gobierno Digital:

- Definir las responsabilidades relacionadas con el manejo de la seguridad, durante el transcurso del año en Salud Sogamoso ESE. Establecer una metodología de gestión de la seguridad clara y estructurada.

- Reducir el riesgo de pérdida, robo o corrupción de información. Garantizar que los usuarios tienen acceso a la información a través medidas de seguridad con la garantía de calidad y confidencialidad. Implementar las auditorías externas para identificar las debilidades del sistema y las áreas a mejorar.
- Garantizar la continuidad de las operaciones necesarias de la empresa tras incidentes de gravedad.
- Cumplir con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Optimizar la gestión de la seguridad de la información con base en la gestión de procesos.
- Definir el plan para la transición de IPv4 a IPv6 .

2. ALCANCE DEL PESI

El PESI tiene como finalidad el diagnóstico, análisis, definición y planeación del manejo de la seguridad de los procesos que se ejecutan en Salud Sogamoso E.S.E. y será actualizado anualmente; estos apoyarán el cumplimiento de los procesos y objetivos propuestos por las diferentes dependencias de la Entidad y está articulado de manera global en relación con la seguridad de la información.

3. MARCO NORMATIVO PESI

Ley 527 de 1999: Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones, así mismo introduce el concepto de equivalente funcional, firma electrónica como mecanismos de autenticidad, disponibilidad y confidencialidad de la información. (CONGRESO NACIONAL, 1999).

CONPES 3670 de 2010. "Lineamientos de Política para la continuidad de los programas de acceso y servicio universal a las Tecnologías de la Información y las Comunicaciones".

CONPES 3701 de 2011. "Lineamientos de Política para Ciberseguridad y Ciberdefensa" Ley 872 de 2003. "Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios".

Ley 1341 de 2009. "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones - TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones".

Ley 39 de 1981. Sobre microfilmación y certificación de archivos.

Ley 594 de 2000. "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. (CONGRESO DE LA, 2014)

Decreto 103 de 2015: Por la cual se reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones, en cuanto a la publicación y divulgación de la información. (PRESIDENCIA DE LA, 2015)

Decreto 2609 de 2012: Por el cual se dictan disposiciones en materia de gestión documental y gestión documental electrónica. (2012)

Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones. (MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS, 2012)

Ley 1273 de 2009: Ley la cual se crea y se protege el bien jurídico de la información y los datos personales.

Ley 1581 de 2012: Ley Estatutaria por la cual se reglamenta el artículo

15 de la Constitución política, relativo a la intimidad personal y el Habeas Data, a través de esta norma se dictan disposiciones generales para la protección de datos personales.

Ley 594 de 2000: Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. (CONGRESO D. L., 2000)

4. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Salud Sogamoso E.S.E. se compromete a un eficiente manejo de la información, utilizando recursos adecuados, apoyados en lineamientos que garanticen la confidencialidad, privacidad, seguridad y confiabilidad de la información.

Salud Sogamoso E.S.E. entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad 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 nuestra entidad.

Salud Sogamoso E.S.E., Tiene riesgos identificados 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.

El contenido de esta política aplica a la entidad según como se defina 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 SGSI 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 usuarios, entes de control 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, practicantes y usuarios de Salud Sogamoso E.S.E.
- Garantizar la continuidad de Salud Sogamoso E.S.E.frente a incidentes.
- Salud Sogamoso E.S.E. Ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la Corporación, y a los requerimientos regulatorios.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de Salud Sogamoso E.S.E.:

• Salud Sogamoso E.S.E. ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades empresariales , y a los requerimientos regulatorios que le aplican a su naturaleza.

• Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

• Salud Sogamoso E.S.E. protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

• Salud Sogamoso E.S.E. protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• Salud Sogamoso E.S.E. protegerá su información de las amenazas originadas por parte del personal.

• Salud Sogamoso E.S.E. protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• Salud Sogamoso E.S.E. controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• Salud Sogamoso E.S.E. Implementará control de acceso a la información, sistemas y recursos de red.

• Salud Sogamoso E.S.E. garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• Salud Sogamoso E.S.E. garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

• Salud Sogamoso E.S.E. garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

• Salud Sogamoso E.S.E. garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas y adoptadas en el MANUAL DE GERENCIA Y SEGURIDAD DE LA INFORMACIÓN.

5. ANÁLISIS DE LA SITUACIÓN ACTUAL

5.1 Análisis de brecha MSIP

Apoyados en la herramienta "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD" se obtuvieron los siguientes resultados de análisis de brecha sobre la efectividad de los controles enero 2020, obteniendo los siguientes resultados:

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD. Ministerio de Tecnologías de la Información y Comunicaciones, borrador 2017

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	26	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	52	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	60	100	EFECTIVO
A.9	CONTROL DE ACCESO	60	100	EFECTIVO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	60	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	80	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	80	100	GESTIONADO

A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	80	100	**GESTIONADO**
A.15	RELACIONES CON LOS PROVEEDORES	40	100	**REPETIBLE**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	80	100	**GESTIONADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40	100	**REPETIBLE**
A.18	CUMPLIMIENTO	60	100	**EFECTIVO**
PROMEDIO EVALUACIÓN DE CONTROLES		**55**	**100**	**EFECTIVO**

En la tabla y grafico anterior Se evidencia que se debe trabar en los siguientes temas:

- Políticas de Seguridad de la Información

- Organización de la seguridad de la información.
- Instrumento de identificación de la línea base de seguridad administrativa y técnica hoja levantamiento de información
- Relaciones con los proveedores
- Aspectos de seguridad de la información de la gestión para la continuidad del negocio

La calificación total es de 51 de 100 la cual es susceptible de evaluación continua.

Gracias a este análisis se priorizan los seis temas anteriores.

En cuanto al análisis de brecha para el avance se diligenciará la matriz PHVA del instrumento de evaluación del MSPI. Con esta herramienta se determinar las acciones a seguir en cada fase del modelo.

En cuanto a la madurez del MSPI se tiene el siguiente análisis:

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%

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

ID REQUISITO	CALIFICACIÓN OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	NIVEL 3 DEFINIDO	CUMPLIMIENTO NIVEL DEFINIDO	NIVEL 4 GESTIONADO CUANTITATIVAMENTE	CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE	NIVEL 5 OPTIMIZADO	CUMPLIMIENTO NIVEL 5 OPTIMIZADO
LIMITE DE MADUREZ INICIAL	360	260	MENOR	440	MENOR	600	MENOR	780	MENOR	980	MENOR
LIMITE DE MADUREZ GESTIONADO	437	0		460	MENOR	660	MENOR	880	MENOR	1100	MENOR
LIMITE DE MADUREZ DEFINIDO	392	0		0		660	MENOR	880	MENOR	1100	MENOR
LIMITE DE MADUREZ GESTIONADO CUANTIT	463	0		0		0		660	MENOR	880	MENOR

ATIVAM ENTE											

De acuerdo al análisis de brecha se priorizan para el año 2020 las actividades faltantes para alcanzar el nivel 3.

- Análisis de brecha Transición de IPv4 a IPv6 se debe gestionar para lograr la transición a 31 de Diciembre del año 2020
- Gestión de Información atendiendo al resultado establecido en la hoja de Madurez del instrumento de evaluación MSPI, en el campo cumplimiento nivel gestionado donde el estado evaluado del ítem esta en grado menor.

G O	S E G	CONTROL DE ACCES	USUARIOS			
			Ciudadanía-EAPB-Gobierno Nacional	Entidades Públicas Privadas – Persona Natural – Comunidades Étnicas – Asociaciones de Usuarios – Comunidad en general – Entes territoriales – Rama judicial - Entes de Control – Cooperación Internacional – Gremios.		
		PRESENTACIÓ	ACCESO A LA INFORMACIÓN			
			Consulta en Línea trámites en CITA y PQRDS– PÁGINA WEB – Boletines y Comunicados – Reportes – Estadísticas – Datos Abiertos –			
		DATA Y	Bodegas de Datos Agrupados			
			Directorio Activo – CNT – Servidores dedicados			
		CONTINUIDAD DEL NEGOCIO	CALIDAD DE DATOS			
			Parámetros databases	Módulo de Metadatos MODULOS ASISTENCIALES Y ADMINISTRATIVOS-	Datos Maestros -información de usuarios	Estándares
		TELECOM UNI	EXTRACCIÓN, TRASFORMACIÓN Y CARGA DE BASES DE DATOS			
			Gestión de Calidad de Datos Formato, completitud, codificación estandarizada			

COMUNICACIÓN Y	SERVICIOS DE INTEROPERABILIDAD (GEL-XML (MIN TIC) / OGC- ICDE))				
	Servicios Intercambio de Negocio		Catálogo de Servicios	ESB – Bus de servicios de Conectividad y Orquestaciones	
PROCESO	CERTIFICACIÓN DE OPERACIONES ESTADÍSTICAS Y/O REGISTROS ADMINISTRATIVOS				
	Lenguaje Común de Intercambio – Mapas de Intercambio -- Calidad de Datos -- Estandarización con modelos de dominios sectoriales – Directorio de Componentes --				
FÍSICA Y	EXTRACCIÓN TRANSFORMACIÓN Y CARGA				
	SQL				
APLICACIONE	SISTEMAS DE INFORMACIÓN				
	CNT, ENTERPRISE, IDENTIFICADOR DE USUARIOS DIGITURNO, MODULO DE VENTANILLA UNICA DE RADICACION. COMPROBADOR DE DERECHOS, PLATAFORMA ASTERIX QUE GESTIONA CALL CENTER, PAGINA WEB, INTRANET.				
POLÍTICA	GOBIERNO DIGITAL	MARCO DE REFERENCIA ARQUITECTURA DE TI	MODELO DE GESTIÓN IT4+	SEGURIDAD DE LA INFORMACIÓN	INTEROPERABILIDAD

6 ANÁLISIS DE RIESGO PARA LA SEGURIDAD DE LA INFORMACIÓN

Se realiza mediante el mapa de riesgos definido para la seguridad de la información en Salud Sogamoso E.S.E.

7 PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Los procedimientos para el cumplimiento de Seguridad y Privacidad de la Información que se tendrán en cuenta en la implementación se definen a continuación.

- Seguridad del recurso humano
- Gestión de activos
- Control de acceso
- Seguridad física y del entorno
- Seguridad de las operaciones

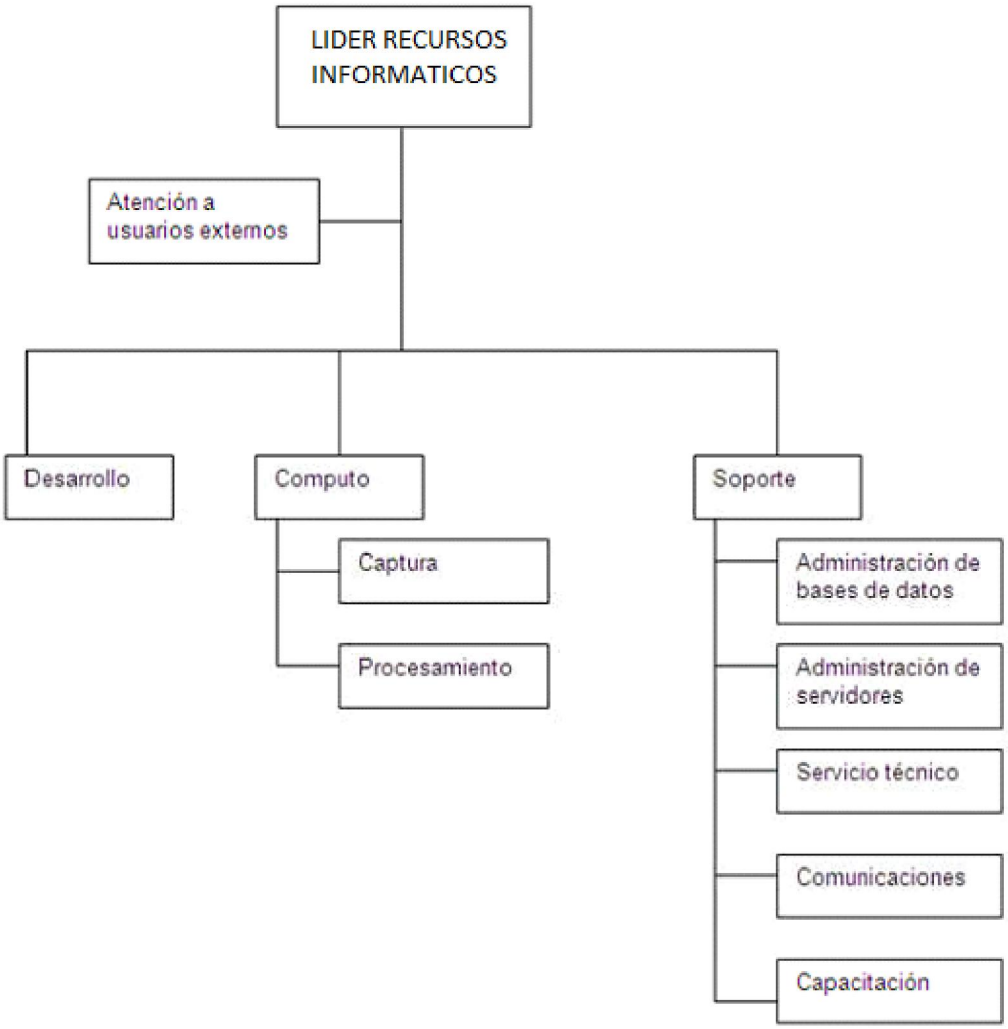
- Seguridad de las comunicaciones
- Relaciones con los proveedores
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información de la gestión de continuidad de empresarial
- Plan de sensibilización y apropiación del MSPI para toda la entidad.

8. ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8.1 Gobierno de SI

Basados en la "Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información" desarrollado por MINTIC y el organigrama de se define el siguiente de SI

Organigrama de SI



8.2 Responsable de Seguridad de la Información:

En Salud Sogamoso se define como responsable de Seguridad de la Información al Líder de Recursos Informáticos.

Por recomendación de la "Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información" se deben desarrollar proyectos de TI y SI, para lo cual la dirección del proyecto está en manos del responsable de SI.

8.3 Equipo del Proyecto:

En la entidad la prestación de los servicios de TI, tales como soporte técnico, página web, Aplicativos como CNT y VALIDADOR DE USUARIOS, etc. Lo tiene el líder de recursos informáticos y el profesional de apoyo, los cuales conforman el equipo para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal a la entidad, y que no dependa exclusivamente de la oficina o área de TI.

Una de las tareas principales del líder del proyecto es entregar y dar a conocer los perfiles y responsabilidades de cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol.

9. PLANEACIÓN DE LAS ACTIVIDADES

POLÍTICAS	JUSTIFICACIÓN	ACTIVIDADES	ene-20	feb-20	mar-20	abr-20	may-20	jun-20	jul-20	ago-20	sep-20	oct-20	nov-20	dic-20
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.	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;				I								
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.	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.				I								

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.	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.												
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.	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.												

Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	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 los usuarios privilegiados con los mecanismos apropiados).												

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.	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.												
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.	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.												

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.	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.											

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.	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.													

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.	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.											

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.	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.													

Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	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.												
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.	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.												

Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	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.											

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.	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 comunicaciones; g) establecer que las instalaciones de procesamiento de información gestionadas por la organización deben estar separadas físicamente de las gestionadas por partes externas.													

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.	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.													
Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	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.													

Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	De acuerdo a la NIST deben identificarse los elementos de resiliencia para soportar la entrega de los servicios críticos de la entidad.											
Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	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.											

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.	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.												

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.	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 para minimizar el riesgo de fuga de información debido a emanaciones electromagnéticas.												

Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	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.												
Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño.	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												

Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	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.											
Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	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											

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.	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.												
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.	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.												
Equipos de usuario desatendidos	Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.	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).												

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.	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.											

Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.	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.													
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.	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).													

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.	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 38de 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													

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.	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; h) definir procedimientos y responsabilidades relacionadas con la protección contra el software malicioso en los sistemas, formación acerca del uso de dichos procedimientos, reporte y recuperación de ataques de software malicioso; i) preparar planes de continuidad del negocio apropiados, para la recuperación de ataques de software malicioso, incluidos todos los datos necesarios, copias de respaldo del software y disposiciones para recuperación; j) implementar procedimientos para recolectar información en forma regular, (la suscripción a listas de correos o la verificación de sitios web que suministran información acerca de nuevo software malicioso); k) implementar procedimientos para verificar información relacionada con el software malicioso, y asegurarse de que los boletines de advertencia sean exactos e informativos; l) alistar entornos en donde se pueden obtener impactos catastróficos.													

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.	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.												

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.	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.												
Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	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.												
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.	Revisar los registros de las actividades del administrador y del operador del sistema, los registros se deben proteger y revisar con regularidad.												

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.	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.												
Instalación de software en sistemas operativos	Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.	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.												

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.	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 secundarios que no se puedan tolerar; si no hay parches disponibles, se debe considerar otros controles como: 1) dejar de operar los servicios o capacidades relacionados con la vulnerabilidad; 2) adaptar o adicionar controles de acceso, (cortafuegos, en los límites de la red); 3) incrementar el seguimiento para detectar ataques reales; 4) tomar conciencia sobre la vulnerabilidad; h) llevar un log de auditoría para todos los procedimientos realizados; i) hacer seguimiento y evaluación regulares del proceso de gestión de vulnerabilidad técnica, con el fin de asegurar su eficacia y eficiencia; j) abordar primero los sistemas que están en alto riesgo; k) establecer un proceso de gestión eficaz de la vulnerabilidad técnica alineada con las actividades de gestión de incidentes para comunicar los datos sobre													

		vulnerabilidades a la función de respuesta a incidentes y suministrar los procedimientos técnicos para realizarse si llegara a ocurrir un incidente; l) definir un procedimiento para hacer frente a una situación en la que se ha identificado una vulnerabilidad, pero no hay una contramedida adecuada. En esta situación, la organización debería evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las acciones de detección y correctivas apropiadas.												
Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Revisar las restricciones y las reglas para la instalación de software por parte de los usuarios.												

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.	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.											
Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	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.											

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.	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.											
Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	De acuerdo a NIST se debe proteger la integridad de las redes incorporando segregación donde se requiera.											

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.	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 no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación incorrecta; k) brindar asesoría al personal acerca de los problemas de usar máquinas o servicios de fax, a saber: 1) acceso no autorizado a almacenes de mensajes built-in para recuperar mensajes; 2) programar las máquinas en forma deliberada o accidental para enviar mensajes a números específicos; enviar documentos y mensajes a un número equivocado, ya sea por marcación errada o por marcar un número almacenado equivocado.												

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.	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.												
Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	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.												

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.	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.												
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.	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).												

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.	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; m) establecer los requisitos de seguros. n) De acuerdo a NIST se deben usar mecanismos de chequeo de las integridad para verificar la integridad del software, firmware, e información													

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.	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.												
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.	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.												

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.	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.												
Revisión técnica de las aplicaciones después de cambios en la plataforma de	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.	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.												

operación													
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.	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.											
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.	Revisar la documentación y los principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.											

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.	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.													

Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	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.												
Pruebas de seguridad de sistemas	Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.	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.												

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.	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.											
Protección de datos de prueba	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	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.											

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.	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 seguridad de la información; 2) el procedimiento que se va a seguir en el caso de un evento de seguridad de la información, (tomar nota inmediatamente de todos los detalles, tales como el tipo de no conformidad o violación, mal funcionamiento, mensajes en la pantalla y reporte inmediato al punto de contacto y realizar solamente acciones coordinadas); 3) referencia a un proceso disciplinario formal establecido para ocuparse de los empleados que cometen violaciones a la seguridad; 4) los procesos de retroalimentación adecuados para asegurar que las personas que reportan eventos de seguridad de la información sean notificadas de los resultados después de que la cuestión haya sido tratada y cerrada.												

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.	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.												
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.	Observe si los eventos son reportados de forma consistente en toda la entidad de acuerdo a los criterios establecidos.												

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.	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.											

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.	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 incidentes es 80												
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.	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.												

Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	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.												
Consolidación y autoevaluación														