INSTITULUA E.I.C.E.

Instituto de Financiamiento, Promoción y Desarrollo de Tuluá

PLAN DE SEGURIDAD Y PRIVACIDAD EN LA INFORMACIÓN MSPI

Enero 2022

ELABORADO POR	REVISADO POR	APROBADO POR
Apoyo Técnico Informática	Profesional Univ. Talento Humano y Servicios Administrativos	Comité Institucional de Gestión y Desempeño

Contenido

1. INTRODUCCIÓN:

Fortalecimiento de la Gestión Pública con TI

Esta iniciativa busca definir una arquitectura TI para consolidar un Estado más articulado, que cuente con mejores capacidades de TI, mejore la calidad y flujo de información en las entidades públicas, y ayude a asegurar que el impacto esperado se alcance de forma oportuna y dentro de los presupuestos planteados.

En este marco de referencia las Instituciones públicas llegan a albergar una gran cantidad de información, bien sea en medios físicos o magnéticos que deben ser salvaguardados de un uso no adecuado por agentes externos a las entidades.

Por lo tanto, es obligación de cada Institución del gobierno tener un plan de seguridad y manejo de la información.

Este documento se elabora con base al taller 1 de Seguridad y Privacidad de la Información que se encuentra en el link http://ticbogota.gov.co/sites/default/files/documentos/Presentacion%20Taller1.pdf , donde hay una agenda a seguir.

También se hace seguimiento al modelo de seguridad y privacidad de la información y 21 guías de trabajo que permite la elaboración del presente documento, con el propósito de definir funciones y asignar responsabilidades en la gestión de la seguridad y privacidad de la información.

2. JUSTIFICACIÓN

El Ministerio TIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones, a través de las cuales contribuye a la construcción de un Estado más eficiente, más

transparente y participativo, publica El Modelo de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea.

Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información en las entidades, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación colombiana.

INFITULUA E.I.C.E. da cumplimiento al Decreto 612 de abril 04 de 2018 Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. En su artículo 2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción.

3. OBJETIVO

3.1. OBJETIVO GENERAL

Generar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para INFITULUA EICE.

3.2. OBJETIVOS ESPECÍFICOS

- Mediante la utilización del Modelo de Seguridad y Privacidad para las Entidades del Estado, se busca contribuir al incremento de la transparencia en la gestión pública.

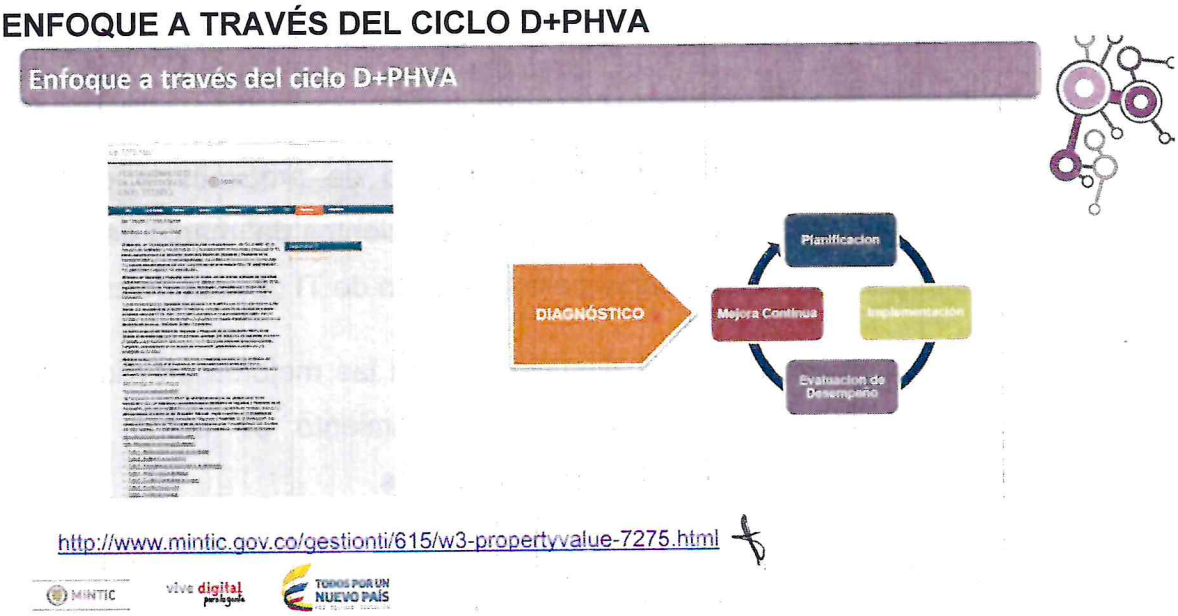
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.

- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Orientar a las entidades en las mejores prácticas en seguridad y privacidad.
- Optimizar la gestión de la seguridad de la información al interior de las entidades.
- Orientar a las entidades en la transición de IPv4 a IPv6 con la utilización de las guías disponibles para tal fin.
- Orientar a las entidades en la adopción de la legislación relacionada con la protección de datos personales.
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones.
- Contribuir en el desarrollo del ejercicio de arquitectura empresarial apoyando en el cumpliendo de los lineamientos del marco de referencia de arquitectura empresarial para la gestión de TI del estado colombiano.
- Orientar a las entidades destinatarias en las mejores prácticas para la construcción de una política de tratamiento de datos personales respetuosa de los derechos de los titulares.
- Optimizar la labor de acceso a la información pública al interior de las entidades destinatarias.

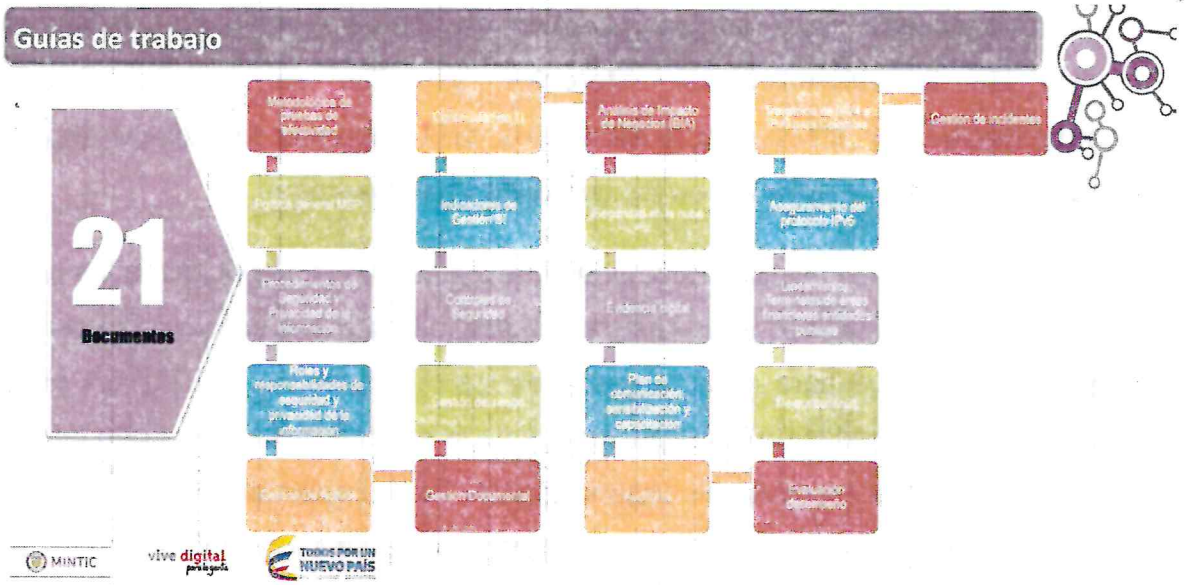
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

4. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN COMPOSICIÓN

5. ENFOQUE A TRAVÉS DEL CICLO D+PHVA



6. GUIAS Y DOCUMENTACIÓN BASE



7. METODOLOGÍA DE PRUEBAS DE EFECTIVIDAD.

INFITULUA EICE. pretende indicar los procedimientos de seguridad que pueden generarse durante el proceso de evaluación en los avances en la implementación del modelo de seguridad y privacidad de la información.

INFITULUA E.I.C.E. adopta un enfoque de seguridad en el cual se incluya el desarrollo y mantenimiento de la misma, realizando mejoras en las áreas que se requiera.

La metodología de pruebas de efectividad es una serie de actividades, que tienen por finalidad comprobar o medir la eficiencia de la implementación del modelo de seguridad en las entidades.

Esta metodología es desarrollada en diferentes etapas que permiten concluir que tanto ha avanzado la entidad con la implementación del modelo; de esta manera, a través de la valoración de diferentes aspectos se permitirá identificar vulnerabilidades y amenazas a las cuales está expuesta la entidad, así como también posibles debilidades en los controles implementados.

Un factor externo de mucho impacto, que se alinea con la ejecución de las pruebas de seguridad y privacidad y sus resultados, son los intereses de lo que se denomina Alta Dirección, que para nuestro caso son los directivos de INFITULUA E.I.C.E., estos se ven reflejados en las capacidades de la entidad de llevar a buen término la implementación del modelo de seguridad para dar cumplimiento a la normatividad vigente; así como llevar a la entidad al siguiente nivel de seguridad que permite que sus procesos y atención al ciudadano deje una buena imagen en la sociedad colombiana.

La metodología busca desde el primer momento de la ejecución, crear una línea base del estado de seguridad de la entidad, es decir, facilitar la identificación de la brecha en la implementación del modelo de seguridad, entiéndase como línea base la primera medición; las siguientes mediciones darán a la entidad la percepción de seguridad que manifiestan en la implementación del modelo de seguridad.

- ✓ **Levantamiento de Información**

En esta fase la entidad debe recopilar la información necesaria para iniciar la actividad, dicha información puede ser organizada por parte del equipo de seguridad de la información de la entidad.

La información recogida no solo debe permitir identificar los activos más importantes de la entidad, relacionados con los procesos de la misma, ya sea misionales o de

apoyo. También me debe permitir el conocer el contexto de la entidad, es decir, el entorno donde se proyectan los objetivos de la entidad.

Por lo tanto, definimos a INFITULUA E.I.C.E. así:

INFITULUA E.I.C.E., En su naturaleza jurídica, es una empresa industrial y comercial del estado, del orden municipal, dotada de personería jurídica, patrimonio independiente y autonomía administrativa. Para todos los efectos legales la entidad podrá usar la sigla INFITULUA E.I.C.E.

En este sentido, INFITULUA E.I.C.E tiene como objeto el fomento y promoción de la competitividad y la productividad en el municipio de Tuluá y otros entes territoriales, a través de la gestión económica y el desarrollo de actividades de administración, financiamiento, comerciales, inmobiliarias e industriales. Así mismo, el instituto podrá atender la ejecución de obras públicas ordenadas dentro de los planes de desarrollo y los planes y programas sectoriales de los entes territoriales en competencia con el sector privado.

En el desarrollo de la recolección de información utilizando el formato "Planilla para la identificación del inventario de información" del Ministerio de Tecnologías de la Información y Comunicaciones, MinTic. Se encuentra un total de 129 activos de información básicos del Instituto.

- ✓ **Identificación de grupos de interés:**

Los responsables de cada área son:

Proceso	Responsable
Planeación	Gerente

Comunicaciones	Jefe Administrativo
Gestión de la Calidad	Jefe Administrativo
Atención al Cliente	Jefe Administrativo
Financiamiento	Director Administrativo y Financiero
Gestión de Proyectos	Gerente
Gestión Financiera	Director Administrativo y Financiero
Gestión de Seguridad y salud en el trabajo	Jefe Administrativo
Gestión de talento humano	Jefe Administrativo
Gestión Documental	Jefe Administrativo
Gestión Ambiental	Jefe Administrativo
Gestión Jurídica	Jefe Oficina Jurídica
Gestión Informática	Jefe Administrativo
Gestión Logística	Jefe Administrativo
Gestión contractual	Jefe Oficina Jurídica
Gestión de Control	Gerente

- ✓ **Mapa de Procesos:**

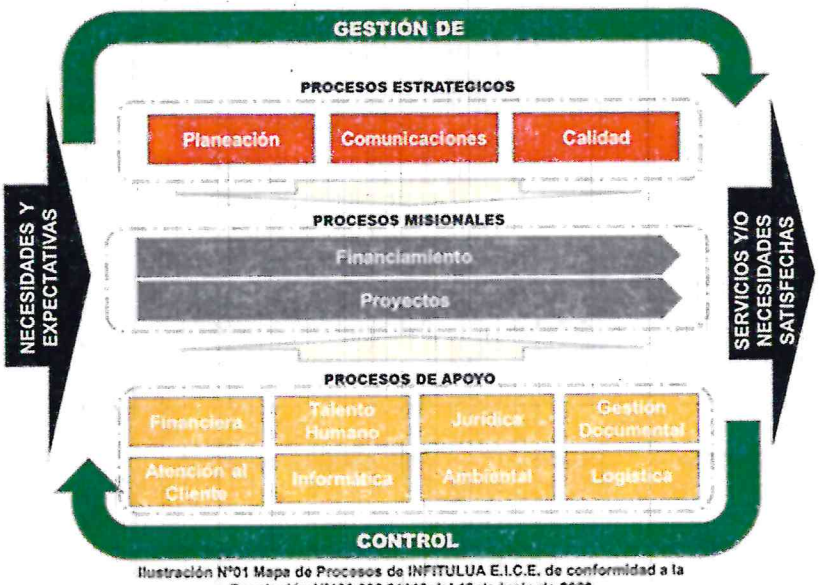


Ilustración N°01 Mapa de Procesos de INFITULUA E.I.C.E. de conformidad a la Resolución N°100.036.01119 del 18 de junio de 2020

✓ **Revisión de Manuales:**

INFITULUA E.I.C.E tiene todos sus manuales revisados y publicados en la página web www.infitulua.gov.co, aunque considera que la revisión y actualización de manuales es un proceso continuo.

1.1 Identificación de amenazas

La identificación de amenazas no es otra cosa que la evaluación del riesgo que se realiza en la entidad, es decir, es la evaluación de las actividades donde se ven involucradas las personas, la infraestructura y los procesos; con el objetivo de identificar las amenazas que se ciernen sobre la entidad.

Las amenazas para INFITULUA E.I.C.E. son las siguientes:

CAUSAS	TIPO DE RIESGO	RIESGO	EFECTOS
No se tiene en cuenta el PETI dentro de la elaboración del presupuesto	Operativo	Ejecución inoportuna a las políticas que se plantean en el Plan Estratégico de Tecnología e Informática del instituto	Obsolescencia de equipos y vulnerabilidad a ataques informáticos
Falta de coordinación entre sistemas y el mantenimiento general de la empresa	Operativo	No contar con un cronograma de mantenimiento preventivo aprobado	Daño de equipo, reprocesos, perdida de información, demora de procesos
Antivirus desactualizado	Operativo	Ataque efectivo de un virus	Pérdida de información
Incumplimiento a las políticas de seguridad informática	Operativo	Manipulación sin autorización a la base de datos del sistema de información	Daño o pérdida de información Detraimiento patrimonial
No tener una frecuencia de realización de back ups	Operativo	No realizar back up a intervalos planificados	Perdida de Información
No tener un control a la instalación de software a través de internet	Operativo	Tener software no legalizado en los equipos de cómputo del instituto	Sanciones por derecho de autor
Fallas en la verificación del documento	Operativo	Clasificar una PQRS de manera inadecuada	Demandas
Desconocimiento de la ley	Operativo	Inexistencia de respuesta de la PQRS en el tiempo de ley	Demandas Sanciones
Demora en la utilización de la herramienta de medición	Operativo	No aplicación oportuna en la encuesta de satisfacción al cliente	No cumplimiento de las expectativas del cliente Clientes insatisfechos Pérdida de clientes
Herramienta de medición de satisfacción mal formulada	Operativo	La herramienta para evaluar la satisfacción del cliente no es efectiva	Reproceso

Aumento de las quejas por parte de los clientes	Operativo	Clientes insatisfechos	Pérdida de clientes
Desconocimiento del portafolio de servicios del Instituto	Operativo	Direccionamiento errado de los clientes	Reproceso
Desconocimiento del portafolio de servicios del Instituto	Operativo	Brindar inadecuada atención al cliente	Pérdida de imagen
Reclamos inadecuados por parte de los clientes con agresiones verbales	Operativo	Exposición de los Servidores Públicos a reclamos y agresiones por parte de los clientes	Daño a la integridad física y moral
Falta de ética Profesional	Operativo	Exigir dinero a cambio de realizar tramites	Sanciones y Demandas
No ejecutar adecuadamente el plan de mercadeo y medios	Operativo	Bajo nivel del reconocimiento de la marca INFITULUA E.I.C.E.	Disminución de la prestación de los servicios
No realizar difusión de los proyectos del instituto en los medios de comunicación	Operativo	No dar a conocer los proyectos y actividades de promoción y desarrollo que realiza el instituto	Pérdida de imagen Bajo nivel de reconocimiento
No seguir los lineamientos impartidos para realizar la rendición	Operativo	No presentar informe de rendición de cuentas a la ciudadanía	Sanciones
Demora en la revisión de documentos de los créditos	Operativo	Demora en los tiempos de desembolso del crédito	Perder clientes Bajo nivel de competencia
Perdida de los recursos para ser sostenible	Operativo	incumplir con el financiamiento de proyectos externos	Incumplimiento del objeto del Instituto
Fallas en el manejo del software al parametrizar los valores del crédito	Operativo	Cometer errores en el software cuando se crea un crédito	Sanciones Perdida económica
No custodiar los documentos debidamente	Operativo	Pérdida de documentos que soportan el crédito, como pagares e hipotecas.	No se pueden realizar los cobros ejecutivos que permitan la recuperación de los recursos económicos.

			Detrimento patrimonial, procesos legales.
Vulnerabilidad de la red	Operativo	hackeo información y robo cibernético en las transacciones monetarias	Perdida económica, investigación .
No verificar datos económicos en la red	Operativo	No actualizar el sistema de información de cartera (DTF) y tasa de usura	Perdida recursos cobrar tasas inapropiadas
Limitación de recursos hídricos para gestionar Proyectos de Infraestructura	Operativo	Restricción Ambiental para ejecutar proyectos	Sanciones e Inv. Disciplinarias. Perdidas Económicas.
Inadecuada Implementación del PGA y Plan de Acción Ambiental	Cumplimiento	Incumplimiento del Marco Legal y Normativo	Sanciones e Inv. Disciplinarias. Pérdidas Económicas.
Restricción de la comunidad para la Ejecución de los proyectos	Operativo	Restricción Ambiental para ejecutar proyectos	Sanciones e Inv. Disciplinarias. Pérdidas Económicas.
Deficiencia en la planeación del proyecto	Operativo	Inadecuada disposición de los residuos de construcción	Sanciones e Inv. Disciplinarias. Pérdidas Económicas.
No asignación del personal idóneo para la ejecución del PAA del proyecto	Cumplimiento	Incumplimiento en la implementación del componente Ambiental del proyecto	Sanciones e Inv. Disciplinarias. Pérdidas Económicas.
Falta de formación para realizar un análisis congruente con la necesidad a contratar	Operativo	Elaboración incorrecta de la solicitud de contratación	Mala interpretación de la labor a contratar. No hay una definición clara del objeto y las actividades a desarrollar por el contratista.
Falta de capacitación	Operativo	Inapropiada estimación de los riesgos en los estudios previos	Pérdida económica Paro de actividades
Desconocimiento de las necesidades del contrato	Operativo	Estimación económica inadecuada del contrato	Sobrecostos Incumplimiento en los objetivos esperados
Desconocimiento de la ley	Operativo	Incumplimiento de los requisitos estipulados por la normatividad vigente	Multas

Mala planeación de los tiempos del contrato	Operativo	Discordancia en los tiempos del contrato	Pérdida económica Paro en las actividades Demora en la entrega de las actividades
No realizar el trámite de la póliza de cubrimiento	Operativo	Inexistencia de la póliza solicitada sin cubrimiento de los amparos requeridos	Pérdida de Tiempo Paro en las actividades
No verificar las garantías en el anexo modificatorio del contrato	Operativo	En las adiciones del contrato no existe el anexo modificatorio de las respectivas garantías	Pérdida económica Pérdida de tiempo Incumplimiento de las actividades
No cumplimiento de las actividades del contrato	Operativo	No cumplir con el objeto del contrato	Pérdida económica Pérdida de tiempo Demora en el cumplimiento de las actividades
Fallas en el seguimiento a los procesos	Operativo	Inexistencia del acto de liquidación del contrato	Falta del paz y salvo Demandas
Fallas en el seguimiento al proceso	Operativo	Inadecuada clasificación de bienes y servicios	Dificultad en el pago de los bienes y servicios
Fallas en el seguimiento al proceso	Operativo	Incumplimiento del cronograma de la invitación pública	Incumplimiento de la ley Sanciones
El funcionario no tiene en cuenta todas las ofertas presentadas al Instituto	Operativo	No incluir una oferta presentada	Demandas Reclamo del oferente
No contar con una verificación de la información por una persona idónea	Operativo	El informe de evaluación no estará acorde con las propuestas presentadas	Selección equivocada del oferente Demanda
Las especificaciones técnicas nos sean adecuadas	Operativo	Realizar los pliegos de condiciones de manera inadecuada	No consecución de un adjudicado Deserción del proceso
Bajos Niveles de Ética y Principios	Estratégico	Compartir Información con terceros en busca de beneficios personal	Perdida Competitiva

Mala planificación de las actividades del sistema integrado de gestión	Operativo	No se identifique eficacia de las acciones del sistema integrado de gestión	Pérdida de imagen
Débil estructuración de la ficha técnica de los indicadores	Operativo	Inadecuada medición de los resultados de la gestión de los procesos	Reprocesos
El personal asignado a la auditoria no cuenta con la información requerida, el personal no se encuentra capacitado. Falta de tiempo	Operativo	Auditorías de Calidad ineficientes	Baja calidad de las auditorías No encontrar evidencias que permitan identificar mejoras en el proceso
No realizar la planeación para la presentación de informes	Operativo	Presentación inoportuna de informes a los entes de control	Sanción fiscal Sanción disciplinaria
Inexistencia de capacitación en Auditorias Auditores sin experiencia	Operativo	Presentación errónea en los informes de auditoria	Mala toma de decisiones
Falta de planeación	Operativo	Realizar auditorías por fuera de los tiempos establecidos	No hay oportunidad de mejora
Falta de formación	Operativo	No contar con un equipo auditor competente para realizar la auditoría	Información no confiable
Falta de formación	Operativo	Elaborar listas de chequeo sin el enfoque que establece el programa de auditoría	Auditoría sin criterios de evaluación
Incumplimiento de las actividades del procedimiento	Operativo	No evaluar el desempeño de los auditores después de un ciclo de auditoría	No hay oportunidad de mejora
Incumplimiento al manual de funciones	Operativo	Coadministración del responsable de Control Interno	Imparcialidad en el control a la gestión
No realizar una mediación donde se ponen de acuerdo las partes que participan en el proyecto	Operativo	Dar inicio a un proyecto sin tener claro los objetivos que se pretenden alcanzar y las partes interesadas que participan	Pérdida de tiempo y recursos

No tener criterios definidos para la selección del ejecutor	Operativo	Incorrecta planificacion y ejecución del proyecto	Pérdida económica
No realizar una correcta planificación financiera	Operativo	No terminar el proyecto	Pérdida económica Pérdida de credibilidad
Mala planificación del proyecto	Operativo	Extender los tiempos planificados para la ejecución del proyecto	Aumento de los costos y gastos del proyecto
No determinar las especificaciones de los productos que se requieren	Operativo	El proyecto no cumpla con las especificaciones y expectativas que establecen las partes	Pérdida de recursos Pérdida de imagen
No se realice un estudio para conocer los beneficios que el proyecto haya generado	Operativo	No se pueda medir el impacto de proyecto	Desconocimiento de la acogida e impacto del proyecto en el entorno
Inadecuada asesoría en gestión documental	Operativo	Mala aplicación de las TRD en las unidades administrativas	Reprocesos Demoras
Inadecuada elaboración de las TRD	Operativo	Mala clasificación de la producción documental de cada unidad administrativa	Demora en la consulta y préstamo de documentos
Falta de control	Operativo	Pérdida de trazabilidad en la distribución de las comunicaciones internas y externas.	Sanciones e investigaciones
Robo, falta de seguridad	Operativo	Pérdida de información fisíca	Sanciones e investigaciones
Desactualización en Leyes y normas del proceso	Operativo	Error en la implementación de normas y leyes en los procedimientos del proceso	Sanciones y Reprocesos
Realizar un plan financiero que no se ajuste a los recursos financieros	Operativo	Inadecuada proyección del plan financiero	Perdida económica Iliquidez
No contar con capacitaciones en temas de reformas normativas	Operativo	Inadecuada aplicación del decreto 1525 del 2008	Investigación

No contar con procedimiento para adquirir las garantías del crédito	Operativo	Ejecutar créditos sin las garantías	perdida económica iliquidez
Depender de terceros	Operativo	Invertir recursos en acciones con volatilidad permanente	iliquidez falta de apalancamiento
Los clientes no cumplan sus obligaciones	Operativo	Baja recuperación y rotación de cartera	Iliquidez Vencimiento de pagares
Desconocimiento de los tiempos para los pagos tributarios	Operativo	Pagos tributarios extemporáneos	Sanciones
No realizar las conciliaciones en el momento de la transacción	Operativo	No conciliar entre presupuesto contabilidad , nomina, tesorería , y activos fijos	Descuadre y cifras no confiables para tomar decisiones
Pasar por alto un adecuada redacción y motivación de un acto administrativo, Contratos y otros pronunciamientos	Operativo	Revisión de un acto administrativo, Contratos y otros pronunciamientos inadecuados	No realizar el debido control legal de los actos administrativos Modificación o derogación del acto administrativo
No realización de las respuestas a los peticionarios en el tiempo establecido por la ley	Operativo	No generar una respuesta de tutelas, acciones de cumplimiento, demandas y derechos de petición en los tiempos establecidos por la ley	Esto conlleva a: Sanción pecuniarias , disciplinarias o penales
Falta de diligencia por parte de la Dirección jurídica	Operativo	Conceptos no conforme a la ley	Actuaciones administrativas con fundamentos legales inadecuados
No verificar los datos consignados en el contrato en concordancia con la póliza	Operativo	Aprobación de pólizas sin previa revisión	Hallazgo de los entes de control Póliza sin cumplimiento de garantías
No revisar los requerimientos del contrato de acuerdo a la ley	Operativo	Inadecuada revisión de la contratación	Sanciones pecuniarias, disciplinarias y penales
No realizar el mantenimiento de los equipos	Operativo	No organizar cronograma de mantenimiento preventivo según las necesidades del Instituto	Pérdida económica

No diligenciar el formato de seguimiento a los equipos	Operativo	Realizar el seguimiento a los equipos muebles y enseres, vehículos de manera inadecuada	Pérdida económica
No hay un control de inventario en las entradas y salidas	Operativo	Pérdida de activos	Pérdida económica Disminución del patrimonio
No tener un inventario con los costos y organización de los equipos	Operativo	No asegurar los muebles inmuebles del Instituto	Perdidas económicas
No controlar la entrada y salida de personas	Operativo	Exposición de la entidad a hurtos	Posible robo a la infraestructura y funcionarios
Estructura orgánica y financiera débil	Operativo	La entidad no cumpla con la operatividad para la cual fue creada	Detrimento patrimonial y cierre de la entidad
Falta de parametrización uniforme en la elaboración de los planes estratégicos y de acción. Desconocimiento de la norma de la planeación estratégica.	Operativo	Incoherencia entre la Misión Institucional, Plan Estratégico, Plan de Acción, Procesos, Procedimientos.	Una entidad sin direccionamiento, sin resultados, desorganización, duplicidad de actividades. Multa/Sanción
Mal diseño de los planes y programas y/o falta de control y seguimiento a los mismos	Operativo	No cumplir con las metas de los planes y programas diseñados	Insuficiencia en los resultados de gestión.
Realizar el pago de la nómina fuera de las fechas establecidas	Operativo	Realizar el pago de la nómina y seguridad social y prestaciones sociales inoportunamente	Reproceso en las actividades a desarrollar de los funcionarios
No hay una evaluación de desempeño	Operativo	Existencia de un personal Inexperto	Errores Operativos o de procedimientos
Errores en procedimientos	Operativo	Fallar en la ejecución del proceso de Talento Humano	Sanciones Multas
Fallas relaciones interpersonales Personal desmotivado	Operativo	Bajo nivel de compromiso con el instituto	Baja productividad en las actividades

No se cumpla con los requisitos del manual de funciones	Estratégico	Mal clima laboral	Malas relaciones laborales
No incluir el reglamento de trabajo en temas de inducción y no entregar copia al servidor publico	Operativo	Incumplimiento del reglamento de trabajo	Desconocimiento de los derechos y deberes como funcionario público
Desconocimiento de la ley	Operativo	Error en la implementación de normas y leyes del proceso	Sanciones y Reprocesos
No contar con una sede propia	Operativo	Dificultad para desarrollar las funciones administrativas de cada Servidor Publico	Incumplimiento misional
Condiciones climáticas y Desastres Naturales	Operativo	Afectación en la continuidad del proyecto	Perdidas económicas, Humanas
Falta de control y seguimiento a la administración de los recursos del proyecto	Operativo	Uso indebido de recursos del proyecto para beneficio personal	Perdidas económicas y e imagen Institucional

Se realiza una matriz para identificar y abordar el riesgo.

- ✓ **Prueba y análisis**

Se realiza prueba sobre el plan de contingencia para recuperar datos desde las copias de seguridad que se tienen en la nube, en un computador completamente formateado.

- ✓ Reporte
- ✓ Informes y recomendaciones

a. POLITICA GENERAL MSPI V1

8. POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Política Corporativa de Seguridad de la Información

En INFITULUA E.I.C.E. la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como

parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales, INFITULUA E.I.C.E. implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en INFITULUA E.I.C.E. ; este proceso será liderado de manera permanente por el Oficial de Seguridad de la Información.

Esta política será revisada con regularidad como parte del proceso de revisión gerencial, o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

Políticas generales de seguridad de la información

INFITULUA E.I.C.E. ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la Institución en cuanto a la protección de sus activos de Información:

- ✓ El Comité Institucional de Gestión y Desempeño, será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información de INFITULUA E.I.C.E.

- ✓ Los activos de información de INFITULUA E.I.C.E., serán identificados y clasificados para establecer los mecanismos de protección necesarios.
- ✓ INFITULUA E.I.C.E. Definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.
- ✓ Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- ✓ Se realizarán auditorías y controles periódicos sobre el modelo de gestión de Seguridad de la Información de INFITULUA E.I.C.E.
- ✓ Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la Institución.
- ✓ Es responsabilidad de todos los funcionarios y contratistas de INFITULUA E.I.C.E. reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

9. PROCEDIMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El conjunto de procedimientos que se presentará a continuación, constituye una base sólida para que INFITULUA E.I.C.E. genere sus documentaciones propias dependiendo de sus características particulares, sus activos de información, sus procesos y los servicios de información que pueda prestar.

Con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad, se tomaron en cuenta los 14 numerales de control de seguridad de la información definidas en la norma ISO/IEC 27001, para definir los procedimientos de seguridad necesarios.

- ✓ **Seguridad del recurso humano**

En INFITULUA E.I.C.E. existe un proceso de inducción y reinducción del personal, con el cual se realizar la capacitación y sensibilización de los empleados en temas de seguridad de la información teniendo en cuenta los diferentes roles y responsabilidades (MN-P31-01 v06 Manual de Inducción y Reinducción)

Su periodicidad en la reinducción no debe superar los dos (2) años, en el cual se aprovecha para explicar los manuales de políticas de seguridad informática, se deja como evidencia el formato FO-P31-06 v06 Control de asistencia a la capacitación.

- ✓ **Procedimiento de Ingreso y desvinculación del personal**

En INFITULUA E.I.C.E. existe un procedimiento PR-31-04 v05 para la vinculación de empleados cuyo objetivo es definir y unificar el mecanismo interno de vinculación de trabajadores oficiales que desempeñaran las funciones establecidas en el contrato de trabajo definido.

En el momento se encuentra en proceso de construcción el procedimiento para la desvinculación de trabajadores oficiales.

- ✓ **Gestión de activos de información**

Para este caso INFITULUA E.I.C.E. utiliza la matriz "planilla para la identificación de activos de información", creación del Ministerio de las tecnologías y la información.

- ✓ **Procedimiento para el acceso seguro de los sistemas de información**

En INFITULUA EICE se ha implementado el formato FO-P35-04 v03 Solicitud de acceso y el formato FO-P31-02 V5 Novedades de personal, ambos son evidencia en el área de sistemas para la creación de accesos, roles y seguimientos de usuarios.

- ✓ **Procedimiento de gestión de usuarios y contraseñas**

INFITULUA EICE, posee un servidor de Active Directory con Windows Server 2008 R2, que permite el uso de contraseñas seguras a través de una directiva de contraseña adecuadas, pero en la actualidad no se encuentra configurado. Hay configuraciones de directiva de contraseña que controlan la complejidad y la duración de las contraseñas, como las contraseñas deben cumplir los requisitos de complejidad configuración de directiva.

Puede configurar las directivas de contraseñas en la siguiente ubicación mediante el uso de la consola de administración de directivas de grupo en el controlador de dominio:

Configuración de equipo\Configuración de Windows\Configuración de seguridad\Directivas Cuenta\directiva

Si los grupos individuales requieren directivas de contraseña distintos, estos grupos deben separarse en otro dominio o bosque, en función de los requisitos adicionales.

Los temas siguientes proporcionan una explicación de la implementación de directivas de contraseña y consideraciones de prácticas recomendadas, ubicación de la directiva, valores predeterminados para el tipo de servidor o el GPO.

- ✓ **Exigir historial de contraseñas**

La configuración de la política Forzar el historial de contraseñas determina la cantidad de contraseñas nuevas únicas que se deben asociar con una cuenta de

usuario antes de poder reutilizar una contraseña anterior. En INFITULUA EICE, el promedio de cambio de contraseña por usuario esta dado por 30 días.

La reutilización de contraseñas es una preocupación importante. Muchos usuarios desean reutilizar la misma contraseña para su cuenta durante un largo período de tiempo. Mientras más tiempo se use la misma contraseña para una cuenta en particular, mayores serán las posibilidades de que un atacante pueda determinar la contraseña a través de ataques de fuerza bruta. Si se requiere que los usuarios cambien su contraseña, pero pueden reutilizar una contraseña anterior, la efectividad de una buena política de contraseñas se reduce enormemente.

Especificar un número bajo para Forzar el historial de contraseñas permite a los usuarios usar continuamente el mismo pequeño número de contraseñas repetidamente. Si no establece también la edad mínima de la contraseña, los usuarios pueden cambiar su contraseña tantas veces como sea necesario para volver a utilizar su contraseña original.

- ✓ **Duración máxima**

La configuración de la política Máxima edad de contraseña determina el período de tiempo (en días) en que se puede usar una contraseña antes de que el sistema requiera que el usuario la cambie. Puede configurar las contraseñas para caducar después de un número de días entre 1 y 999, o puede especificar que las contraseñas nunca caduquen estableciendo el número de días en 0. Si la edad máxima de la contraseña es entre 1 y 999 días, la edad mínima de la contraseña debe ser menos de la edad máxima de contraseña. Si la edad máxima de la contraseña se establece en 0, la antigüedad mínima de la contraseña puede ser cualquier valor entre 0 y 998 días.

- ✓ **Vigencia mínima de contraseña**

La configuración de la política Edad mínima de la contraseña determina el período de tiempo (en días) en que se puede usar una contraseña antes de que el sistema requiera que el usuario la cambie. Puede configurar las contraseñas para caducar después de un número de días entre 1 y 999, o puede especificar que las contraseñas nunca caduquen estableciendo el número de días en 0. Si la edad máxima de la contraseña es entre 1 y 999 días, la edad mínima de la contraseña debe ser menos de la edad máxima de contraseña. Si la edad máxima de la contraseña se establece en 0, la antigüedad mínima de la contraseña puede ser cualquier valor entre 0 y 998 días.

- ✓ **Longitud mínima de la contraseña**

La configuración de directiva Mínimo de longitud de contraseña determina la menor cantidad de caracteres que pueden formar una contraseña para una cuenta de usuario. Puede establecer un valor de entre 1 y 14 caracteres, o puede establecer que no se requiere contraseña estableciendo el número de caracteres en 0. Para INFITULUA EICE la longitud mínima es de 8 caracteres.

- ✓ **Contraseña debe cumplir los requisitos de complejidad**

Las contraseñas deben cumplir con los requisitos de complejidad. La configuración de la política determina si las contraseñas deben cumplir una serie de pautas que se consideran importantes para una contraseña segura. La habilitación de esta configuración de directiva requiere que las contraseñas cumplan con los siguientes requisitos:

Las contraseñas no pueden contener el valor samAccountName (nombre de la cuenta) del usuario ni el displayName total (valor de nombre completo). Ambos controles no distinguen entre mayúsculas y minúsculas.

SamAccountName se comprueba en su totalidad solo para determinar si forma parte de la contraseña. Si el samAccountName tiene menos de tres caracteres, se omite esta comprobación.

La displayName se analiza para delimitadores: comas, puntos, guiones o guiones, guiones bajos, espacios, signos de libra y pestañas. Si se encuentra alguno de estos delimitadores, el displayName se divide y todas las secciones analizadas (tokens) se confirman para que no se incluyan en la contraseña. Los tokens que tienen menos de tres caracteres se ignoran y las subcadenas de los tokens no se verifican. Por ejemplo, el nombre "Erin M. Hagens" se divide en tres tokens: "Erin", "M" y "Hagens". Como el segundo token tiene solo un carácter, se ignora. Por lo tanto, este usuario no podría tener una contraseña que incluyera "erin" o "hagens" como una subcadena en ninguna parte de la contraseña.

- La contraseña contiene caracteres de tres de las siguientes categorías:
- Letras mayúsculas de idiomas europeos (de la A a la Z, con signos diacríticos, caracteres griegos y cirílicos)
- Letras minúsculas de idiomas europeos (de la a a la z, sharp-s, con signos diacríticos, caracteres griegos y cirílicos)
    - Base 10 dígitos (0 a 9)
    - Caracteres no alfanuméricos: ~! @ # $% ^ & * _- + = `| () {} [] :;" '<>,.? / +

- Cualquier carácter Unicode que esté categorizado como un carácter alfabético, pero no mayúscula o minúscula. Esto incluye caracteres Unicode de idiomas asiáticos.

Los requisitos de complejidad se aplican cuando las contraseñas se cambian o se crean.

La habilitación del Passfilt.dll predeterminado puede ocasionar algunas llamadas al servicio de asistencia técnica adicionales para las cuentas bloqueadas, ya que es posible que los usuarios no estén acostumbrados a tener contraseñas que contengan caracteres distintos a los que se encuentran en el alfabeto. Sin embargo, esta configuración de política es lo suficientemente liberal como para que todos los usuarios puedan cumplir con los requisitos con una curva de aprendizaje menor.

Las configuraciones adicionales que se pueden incluir en un Passfilt.dll personalizado son el uso de caracteres que no sean de la fila superior. Los caracteres de la fila superior son aquellos que se escriben manteniendo presionada la tecla MAYÚS y escribiendo cualquiera de los dígitos del 1 al 10

✓ **Seguridad física del entorno.**

Toda persona que ingresa como usuario nuevo a INFITULUA E.I.C.E., para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

✓ **Usuarios Nuevos**

Todo el personal nuevo de la Institución, deberá ser notificado a la Unidad Administrativa de Sistemas, con el formato FO-P31-02 V05 NOVEDADES DE PERSONAL, para asignarle los derechos correspondientes (Equipo de Cómputo, Creación de Usuario para la Red (Perfil de usuario en el Directorio Activo) o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático.

- ✓ **Obligaciones De Los Usuarios**

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.

- ✓ **Capacitación En Seguridad Informática**

Todo servidor o funcionario nuevo en INFITULUA E.I.C.E. deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática, Manual de

Usuarios, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

- ✓ **Sanciones**

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial, o de que se le declare culpable de un delito informático.

- ✓ **Seguridad Física y Medio Ambiente**

Protección de la Información y Bienes Informáticos

Para el acceso a los sitios y áreas restringidas se debe notificar a la Unidad Administrativa de Sistemas para la autorización correspondiente, y así proteger la información y los bienes informáticos.

Reporte de Riesgo

El usuario o funcionario deberán reportar de forma inmediata a la Unidad Administrativa de Sistemas cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

Unidades de Almacenamiento

El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

Fuga de Información

Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

10. CONTROLES DE ACCESO FÍSICO

- ✓ **Entrada y Salida de Equipos Particulares**

Cualquier persona que tenga acceso a las instalaciones de INFITULUA E.I.C.E., deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad

de la entidad, en Recepción, en el momento de retirar el equipo de las Instalaciones de INFITULUA E.I.C.E., deberá reportar la novedad nuevamente a Recepción, quien revisará en sus archivos el momento de entrada y registrará el momento de salida del activo, también dará un visto bueno de salida.

- ✓ **Entrada y Salida de Equipos De La Entidad.**

Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información perteneciente a INFITULUA E.I.C.E., siempre debe entrar primero al área de inventarios, donde se registrará en el Software Contable, después será asignado a algún funcionario dependiendo de la necesidad, podrá ser retirado de las instalaciones de INFITULUA E.I.C.E.,. Se debe diligenciar el formato F-405-04 . con sus respectivas firmas.

- ✓ **Seguridad en Unidades Administrativas**

Las Unidades Administrativas que componen a INFITULUA E.I.C.E., son áreas restringidas, por lo que solo el personal responsable de su Unidad ó el personal autorizado por la Unidad Administrativa de Sistemas (solo para tareas de prevención o correctivo) puede acceder a los diferentes equipos de cómputo.

11. PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS

- ✓ **Traslados de Equipos**

Los funcionarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Unidad Administrativa de Sistemas, en caso de requerir este servicio, deberá solicitarlo.

- ✓ **Responsabilidad del Hardware**

El Auxiliar Administrativo de Inventarios de activos será el encargado de generar el resguardo y recabar la firma del funcionario a quien se le asigne un equipo de cómputo, como responsable de los activos informáticos que se le establezcan y de conservarlos en la ubicación autorizada por la Unidad Administrativa de Sistemas.

- ✓ **Responsabilidad de la Función del Equipo**

INFITULUA E.I.C.E., será quien ponga a disposición de los usuarios los medios y equipos informáticos para el cumplimiento de sus obligaciones laborales. En consecuencia, dichos equipos informáticos no están destinados al uso personal o extra profesional de los usuarios, por tanto, estos deben de conocer que no gozan del uso privativos de los mismos.

12. CAPACITACIÓN DE HERRAMIENTAS INFORMÁTICAS

Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

- ✓ **Guardar Información**

Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro c:\Mis Documentos, es responsabilidad del Técnico Administrativo en Sistemas re direccionar esta carpeta al servidor principal.

- ✓ **Recomendación De No Ingerir Bebidas O Comida Cerca A Los Equipos Informáticos**

Mientras se esté cerca a el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

- ✓ **Recomendación de no Colocar Objetos sobre los Equipos de Cómputo.**

Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU.

- ✓ **Condiciones Ambientales para el Equipo de Cómputo**

Se debe mantener el equipo informático en un lugar limpio y sin humedad.

- ✓ **Cables de Conexión**

El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar una reubicación de cables con el personal de la Unidad Administrativa de Sistemas

- ✓ **Abstención de Abrir los Equipos de Computo**

Queda terminantemente prohibido que el usuario o funcionario distinto al personal de la Unidad Administrativa de Sistemas abra o destape los equipos de cómputo. No se podrá acceder físicamente al interior de los PC´s.

- ✓ **Procedimiento de gestión de incidentes:**

Los funcionarios de INFITULUA E.I.C.E., están obligados a notificar cualquier incidencia o anomalía en el uso de medios informáticos que detecten: perdida de información, de listados, accesos no autorizados, uso de su identificador de usuario ó de su contraseña, introducción de virus, recuperación de datos, desaparición de

soportes informáticos y, en general, toda situación que pueda comprometer el buen uso y funcionamiento de los sistemas de información.

13. OBLIGACIÓN DEL FUNCIONARIO

El usuario o funcionario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo a la UNIDAD Administrativa de Sistemas lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

- ✓ **De la Información Confidencial**

Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las Directivas Administrativas competentes, el usuario o funcionario informático deberá notificar a la Dirección Financiera y Administrativa de INFITULUA E.I.C.E..

14. INCIDENTES CON ACTIVOS TÉCNOLÓGICOS

Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de INFITULUA E.I.C.E., debe ser reportado a la Unidad Administrativa de Sistemas.

- ✓ **Base de Conocimiento - Control de Incidentes**

Es obligación del Técnico Administrativo llevar un libro de control de incidentes.

- ✓ **Continuidad de negocio:**

El Plan está orientado a establecer, junto con otros trabajos de seguridad, un adecuado sistema de seguridad física y lógica en prevención de desastres.

Se define la Seguridad de Datos como un conjunto de medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o antrópicos. Se ha considerado que para, la información es uno de los activos más importantes, lo cual hace que la protección de esta sea el fundamento más trascendental de este Plan de Contingencia.

En este documento se resalta la necesidad de contar con estrategias que permitan realizar: Análisis de Riesgos, de Prevención, de Emergencia, de Respaldo y recuperación para enfrentar algún desastre. Por lo cual, se debe tomar como Guía para la definición de los procedimientos de seguridad de la Información.

Un Plan de Continuidad de Negocio se compone de varias fases que comienzan con un análisis de los procesos que componen la organización. Este análisis servirá para priorizar qué procesos son críticos para el negocio y establecer una política de recuperación ante un desastre. Por cada proceso se identifican los impactos potenciales que amenazan la organización, estableciendo un plan que permita continuar con la actividad empresarial en caso de una interrupción.

Un Plan de Continuidad de Negocio, a diferencia de una Plan de Contingencia, está orientado al mantenimiento del negocio de la organización, con lo que priorizará las operaciones de negocio críticas necesarias para continuar en funcionamiento después de un incidente no planificado.

En el desarrollo de un Plan de Continuidad de Negocio existen dos preguntas clave:

> ¿Cuáles son los recursos de información relacionados con los procesos críticos del negocio de la compañía?
>
> ¿Cuál es el período de tiempo de recuperación crítico para los recursos de información en el cual se debe establecer el procesamiento del

negocio antes de que se experimenten pérdidas significativas o aceptables?

Un Plan de Continuidad reducirá el número y la magnitud de las decisiones que se toman durante un período en que los errores pueden resultar mayores. El Plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas y procedimientos, acuerdos con entidades internas y externas.

La activación de un Plan de Continuidad debería producirse solamente en situaciones de emergencia y cuando las medidas de seguridad hayan fallado.

15. BENEFICIOS

- Identifica los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto financiero, humano y de reputación sobre la organización.
- Obliga a conocer los tiempos críticos de recuperación para volver a la situación anterior al desastre sin comprometer al negocio.
- Previene o minimiza las pérdidas para el negocio en caso de desastre.
- Clasifica los activos para priorizar su protección en caso de desastre.
- Aporta una ventaja competitiva frente a la competencia.
- Fomenta e implica a los recursos humanos de la compañía en las actividades de continuidad.

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

INFITULUA EICE presenta el siguiente cuadro de Roles y Responsabilidades para el área de sistemas:

DOMINIO	RESPONSABILIDADES	RESPONSABLES
SERVICIOS TECNOLÓGICOS	* Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. * Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. * Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. * Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. * Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. * Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.	APOYO TÉCNICO EN SISTEMAS

ESTRATEGIA TI	* Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.	APOYO TÉCNICO EN SISTEMAS
SISTEMAS DE INFORMACIÓN	* Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. * Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. * Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. * Liderar el proceso de gestión de incidentes de seguridad así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. * Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.	APOYO TÉCNICO EN SISTEMAS
DE INFORMACIÓN	* Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. * Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.	APOYO SISTEMAS MEDIOS DE INFORMACIÓN, APOYO SISTEMAS WEB MASTER

USO Y APROPIACIÓN	* Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. * Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. * Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.	APOYO TÉCNICO DE SISTEMAS, APOYO SISTEMAS MEDIOS DE INFORMACIÓN, APOYO SISTEMAS WEB MASTER

Como instancia orientadora de la implementación de la estrategia de Gobierno en línea de acuerdo al señalado en el Art. 2.2.9.1.2.4. Responsable de orientar la implementación de la Estrategia de Gobierno en Línea. La Institución prevé que las funciones de este comité pueden ser incluidas por el comité Institucional de desarrollo administrativo.

17. GESTIÓN DE ACTIVOS

La Institución cuenta con un plan de gestión de activos actualizado.

✓ **Continuidad de Ti**

La gestión de la continuidad del negocio, es un proceso para holístico a través del cual se identifican los impactos potenciales que amenazan la continuidad de las actividades de las Entidades, proveyendo un marco de referencia para la construcción de la resiliencia y la capacidad de una respuesta efectiva, que le permita proteger los intereses de las Entidades debido a disrupciones.

✓ **Objetivos**

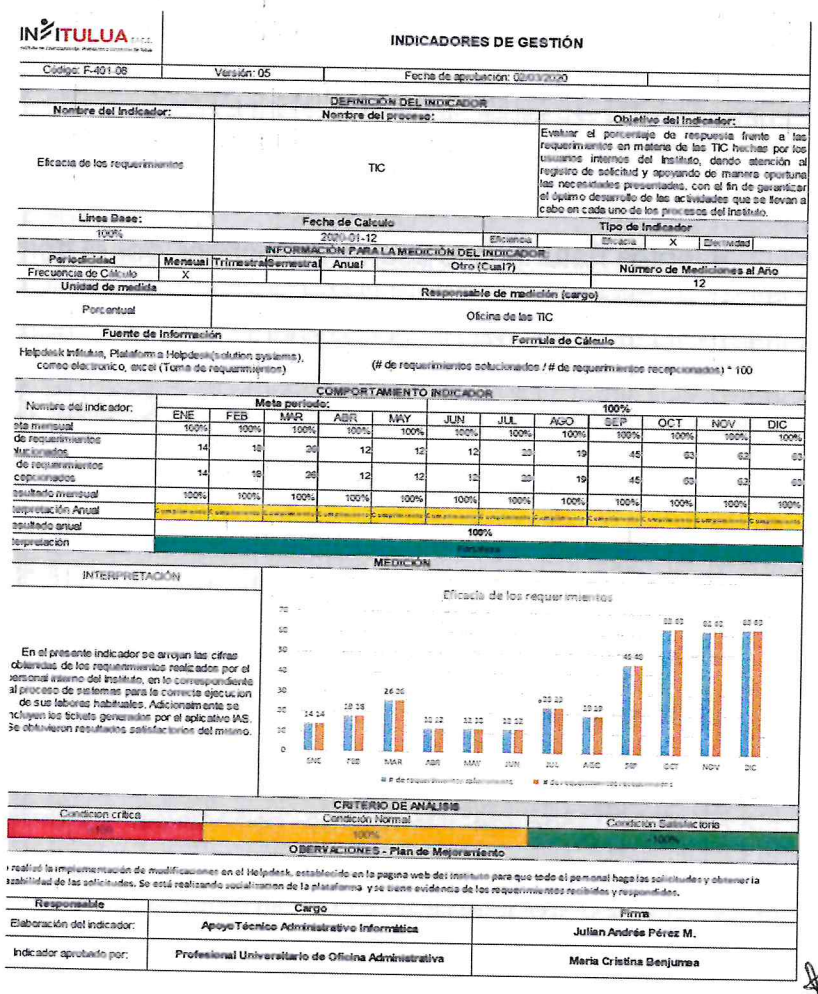
Para lograr esta visión, se han adoptado los siguientes objetivos:

- Establecer procedimientos específicos que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones críticas del negocio que se puedan ver comprometidas por eventos naturales, o sean ocasionados por el hombre.
- Identificar las aplicaciones y las plataformas consideradas críticas para la operación del negocio.
- Identificar al personal clave interno y externo requerido para la operación de las actividades críticas del negocio.
- Establecer los tiempos mínimos de recuperación requeridos en los que no se vea afectado el negocio.
- Definir la funcionalidad mínima que requiere el negocio en caso de contingencia.
- Identificar los riesgos presentes para la continuidad.
- Establecer los elementos esenciales requeridos en el plan de recuperación de desastres.

- Desarrollar procedimientos específicos y guías de operación en caso de desastre para cada uno de los servicios críticos vitales especificados en el alcance del plan.
- Desarrollar e impartir la capacitación inicial para el correcto funcionamiento del plan.
- Establecer un plan de prueba, gestión y mantenimiento necesarias para garantizar los objetivos del Plan.

18. INDICADORES DE GESTIÓN TI

Indicador Porcentaje de cumplimiento del Plan Estratégico de Tecnologías de Información - PETI. Controlar el porcentaje de iniciativas planeadas, relacionadas y ejecutadas en el PETI.



INSTITULUA E.I.C.E.

INDICADORES DE GESTIÓN

Código: F-401.08	Versión: 05	Fecha de aprobación: 02/03/2020

DEFINICIÓN DEL INDICADOR

Nombre del Indicador:	Nombre del proceso:	Objetivo del Indicador:
Eficacia de los requerimientos	TIC	Evaluar el porcentaje de respuesta frente a las requerimientos en materia de las TIC hechas por los usuarios internos del Instituto, dando atención al registro de solicitud y apoyando de manera oportuna las necesidades presentadas, con el fin de garantizar el óptimo desarrollo de las actividades que se llevan a cabo en cada uno de los procesos del Instituto.

Linea Base:	Fecha de Calculo	Tipo de Indicador				
100%	2020-01-12	Eficiencia		Eficacia	X	Efectividad

INFORMACIÓN PARA LA MEDICIÓN DEL INDICADOR

Periodicidad	Mensual	Trimestral	Semestral	Anual	Otro (Cual?)	Número de Mediciones al Año
Frecuencia de Cálculo	X					12

Unidad de medida	Responsable de medición (cargo)
Porcentual	Oficina de las TIC

Fuente de Información	Formula de Cálculo
Helpdesk Institulua, Plataforma Helpdesk(solution systems), correo electronico, excel (Forma de requerimiento)	(# de requerimientos solucionados / # de requerimientos recepcionados) * 100

COMPORTAMIENTO INDICADOR

Nombre del indicador:	Meta periodo:								100%			
	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
ta mensual	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
de requerimientos uucionados	14	18	26	12	12	12	20	19	45	63	63	63
de requerimientos cepcionados	14	18	26	12	12	12	20	19	45	63	63	63
esultado mensual	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
terpretación Anual	Cumplimiento	Cumplimiento	Cumplimiento	Cumplimiento	Cumplimiento	Cumplimiento	Cumplimiento	Cumplimiento	Cumplimiento	Cumplimiento	Cumplimiento	Cumplimiento
esultado anual	100%											
terpretación	Satisfactoria											

MEDICIÓN

INTERPRETACIÓN

En el presente indicador se arrojan las cifras obtenidas de los requerimientos realizados por el personal interno del Instituto, en lo correspondiente al proceso de sistemas para la correcta ejecución de sus labores habituales. Adicionalmente se incluyen los tickets generados por el aplicativo IAS. Se obtuvieron resultados satisfactorios del mismo.

CRITERIO DE ANALISIS

Condicion critica	Condición Normal	Condición Satisfactoria
0%	100%	100%

OBERVACIONES - Plan de Mejoramiento

realizó la implementación de modificaciones en el Helpdesk, establecido en la pagina web del instituto para que todo el personal haga las solicitudes y observar la estabilidad de las solicitudes. Se está realizando socializaciones de la plataforma y se tiene evidencia de los requerimientos recibidos y respondidos.

Responsable	Cargo	Firma
Elaboración del indicador:	Apoyo Técnico Administrativo Informática	Julian Andrés Pérez M.
Indicador aprobado por:	Profesional Universitario de Oficina Administrativa	Maria Cristina Benjumea

19. CONTROLES DE SEGURIDAD

✓ **Objetivo General**

Proteger la información de INFITULUA EICE, los mecanismos utilizados para el procesamiento de la información, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

✓ **Objetivos Específicos**

Establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información dentro de INFITULUA EICE.

Fomentar la consulta y cooperación con organismos especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos a la información propiedad de las entidades del Estado.

Se realiza la siguiente tabla de objetivos y controles con base al documento ISO 27001

Objeto y campo de aplicación		Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI
Referencias normativas		La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación
Términos y definiciones		Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.

Estructura de la norma		La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles.

DOMINIO 1: Políticas de seguridad de la información

OBJETIVO		CONTROL	
Directrices establecidas por la dirección para la seguridad de la información	Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	Políticas para la seguridad de la información	Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
		Revisión de las políticas para seguridad de la información	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.

DOMINIO 2: Organización de la seguridad de la información

Organización interna	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.	Roles y responsabilidades para la seguridad de información	Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
		Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
		Contacto con las autoridades	Se deberían mantener los contactos apropiados con las autoridades pertinentes.
		Contacto con grupos de interés especial	Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
		Seguridad de la información en la gestión de proyectos	La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto

DOMINIO 3: Seguridad de los recursos humanos

Antes de asumir el empleo	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
		Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
Durante la ejecución del empleo	Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	Responsabilidades de la dirección	La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
		Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo
		Proceso disciplinario	Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
Terminación o cambio de empleo	Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.

DOMINIO 4 Gestión de activos

		Inventario de activos	Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos
Responsabilidad por los activos	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.	Propiedad de los activos	Los activos mantenidos en el inventario deberían tener un propietario
		Uso aceptable de los activos	Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
		Devolución de activos	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
		Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
		Etiquetado de la información	Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
Clasificación de la información	Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización	Manejo de activos	Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización
		Gestión de medios removibles	Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
		Disposición de los medios	Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales
		Transferencia de medios físicos	Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte

DOMINIO 5: Control de acceso

Requisitos del negocio para control de acceso	Limitar el acceso a información y a instalaciones de procesamiento de información	Política de control de acceso	Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
		Política sobre el uso de los servicios de red	Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente
Gestión de acceso de usuarios	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	Registro y cancelación del registro de usuarios	Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso
		Suministro de acceso de usuarios	Se debería 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
		Gestión de derechos de acceso privilegiado	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
		Gestión de información de autenticación secreta de usuarios	La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
		Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares
		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 deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios
Responsabilidades de los usuarios	Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.	Uso de la información de autenticación secreta	Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta
Control de acceso a sistemas y aplicaciones	Evitar el acceso no autorizado a sistemas y aplicaciones	Restricción de acceso 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.
		Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
		Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
		Uso de programas utilitarios privilegiados	Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
		Control de acceso a códigos fuente de programas	Se debería restringir el acceso a los códigos fuente de los programas.

DOMINIO 6: Criptografía

Controles criptográficos	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información	Política sobre el uso de controles criptográficos	Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información
		Gestión de llaves	Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida

DOMINIO 7: Seguridad física y del entorno

Áreas seguras	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	Perímetro de seguridad física	Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información
		Controles físicos de entrada	Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
		Seguridad de oficinas, recintos e instalaciones	Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
		Protección contra amenazas externas y ambientales	Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
		Trabajo en áreas seguras	Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
		Equipos	Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización
		Ubicación y protección de los equipos	Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
		Servicios de suministro	Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro
		Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
		Mantenimiento de equipos	Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas
		Retiro de activos	Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
		Seguridad de equipos y activos fuera de las instalaciones	Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
		Disposición segura o reutilización de equipos	Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobreescrito en forma segura antes de su disposición o reutilización.
		Equipos de usuario desatendidos	Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada
		Política de escritorio limpio y pantalla limpia	Se debería 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

DOMINIO 8: Seguridad de las operaciones

Procedimientos operacionales y responsabilidades	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	Procedimientos de operación documentados	Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
		Gestión de cambios	Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
		Gestión de capacidad	Para asegurar el desempeño requerido del sistema sedebería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura
		Separación de los ambientes de desarrollo, pruebas y operación	Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	Controles contra códigos malicioso	Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
Copias de respaldo	Proteger contra la perdida de datos	Respaldo de información	Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada
Registro y seguimiento	Registrar eventos y generar evidencia.	Registro de eventos	Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
		Protección de la información de registro	Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
		Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían 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 deberían sincronizar con una única fuente de referencia de tiempo.
Control de software operaciona	Asegurar la integridad de los sistemas operacionales.	Instalación de software en sistemas operativos	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos
Gestión de la vulnerabilidad técnica	Prevenir el aprovechamiento de las vulnerabilidades técnicas	Gestión de las vulnerabilidades técnicas	Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado
		Restricciones sobre la instalación de software	Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
Consideraciones sobre auditorías de sistemas de informació	Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.	Información controles de auditoría de sistemas	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.

DOMINIO 9: Seguridad de las comunicaciones

Gestion de la seguridad de las redes	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	Controles de redes	Las redes se deberian gestionar y controlar para proteger la información en sistemas y aplicaciones
		Seguridad de los servicios de red	Se deberian 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.
		Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deberian separar en las redes.
Transferencia de información	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	Políticas y procedimientos de transferencia de información	Se deberia 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.
		Acuerdos sobre transferencia de información	Los acuerdos deberian tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
		Mensajeria electrónica	Se deberia proteger adecuadamente la información incluida en la mensajeria electronica
		Acuerdos de confidencialidad o de no divulgación	Se deberian 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.
Requisitos de seguridad de los sistemas de información	Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que presten servicios en redes públicas.	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deberian incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
		Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se deberia proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
		Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se deberia 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.
Seguridad en los procesos de desarrollo y soporte	Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	Politica de desarrollo seguro	Se deberian establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
		Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida del desarrollo se deberian controlar mediante el uso de procedimientos formales de control de cambios.
		Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deberian revisar las aplicaciones criticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
		Restricciones en los cambios a los paquetes de software	Se deberian desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberian controlar estrictamente.
		Principios de construcción de sistemas seguros	Se deberian establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información
		Ambiente de desarrollo seguro	Las organizaciones deberian 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.
		Desarrollo contratado externamente	La organización deberia supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
		Pruebas de seguridad de sistemas	Durante el desarrollo se deberian llevar a cabo pruebas de funcionalidad de la seguridad.
		Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberian establecer programas de prueba para aceptación y criterios de aceptación relacionados.
Datos de prueba	Asegurar la protección de los datos usados para pruebas.	Protección de datos de prueba	Los datos de ensayo se deberian seleccionar, proteger y controlar cuidadosamente
		Relación con los proveedores	
		Seguridad de la información en las relaciones con los proveedores	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores
		Politica de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberian acordar con estos y se deberian documentar.
		Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deberian establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
		Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deberian incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

DOMINIO 10: Gestión de incidentes de seguridad de la información

Gestión de la prestación de servicios con los proveedores	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
		Gestión de cambios en los servicios de proveedores	Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
Gestión de incidentes y mejoras en la seguridad de la información	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.	Responsabilidad y procedimientos	Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
		Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
		Reporte de debilidades de seguridad de la información	Se debería 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.
		Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
		Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
		Recolección de evidencia	La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

DOMINIO 11: Aspectos de seguridad de la información de la gestión de continuidad de negocio

Continuidad de seguridad de la información	La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.	Planificación de la continuidad de la seguridad de la información	La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
		Implementación de la continuidad de la seguridad de la información	La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
		Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.
Redundancias	Asegurar la disponibilidad de instalaciones de procesamiento de información	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Dominio 12: Cumplimiento

Cumplimiento de requisitos legales y contractuales	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
		Derechos de propiedad intelectual	Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
		Protección de registros	Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
		Privacidad y protección de datos personales	Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes
		Reglamentación de controles criptográficos	Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes
Revisiones de seguridad de la información	Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
		Cumplimiento con las políticas y normas de seguridad	Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
		Revisión del cumplimiento técnico	Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información

20. GESTIÓN DEL RIESGO.

Ver mapa de riesgos de la Institución.

21. GESTIÓN DOCUMENTAL.

En INFITULUA EICE existe un manual actualizado de Gestión Documental.

- ✓ **Análisis De Impacto del Negocio (Bia)**

La Gestión del plan de impacto del negocio en las entidades del estado debe responder a una variedad de políticas de restablecimiento de actividades y servicios que apoyen el normal funcionamiento de las infraestructuras de TI y minimicen al máximo las interrupciones o fallas presentadas dentro de la organización. Las entidades deben permanentemente monitorear y reconocer las amenazas más importantes de incidentes que afecten la normal operatividad de los servicios y los sistemas, de tal manera que se debe garantizar la continuidad del negocio a través de mecanismos de recuperación previamente probados y ajustados y que respondan en el menor tiempo posible a las soluciones de los problemas de interrupción generados.

El fin de la implementación del plan de continuidad de TI, es la protección y recuperación de los servicios críticos que se vean afectados por desastres naturales o interrupciones del servicio ocasionadas ya sea por los sistemas de información y comunicación o ya sean por el hombre en virtud de acciones involuntarias o para beneficio propio.

Así mismo, el análisis de impacto de negocios debe convertirse en una herramienta para minimizar los riesgos de indisponibilidad de los servicios e infraestructuras de TI, que afectan las operaciones regulares de las organizaciones, por lo consiguiente debe formar parte de un sistema de gestión de riesgos, que sea utilizado como mecanismo de control para ejecutar tareas de monitoreo de crisis, planes de contingencia, capacidad de marcha atrás y prevención y atención de emergencias.

Las entidades deben contar con un plan de continuidad de Tecnología de Información, que le permita a la organización continuar con sus operaciones, en caso de presentarse fallas o inconvenientes en sus sistemas que le impidan el normal funcionamiento de los servicios de TI, de esta manera, la correcta

implementación del plan deberá permitir restaurar en el menor tiempo posible las operaciones de la entidad.

El análisis de impacto del negocio – BIA por sus siglas en inglés (Bussiness Impact Analysis), está determinado por la construcción de un plan de continuidad del negocio para cada organización, que le permita a cada entidad continuar funcionando a pesar de un desastre ocurrido; el documento generado en este análisis deberá cumplir con lo expuesto en los requerimientos de la ISO/IEC 2700, de este modo el documento BIA debe ser validado e implementado bajo las directrices de cada organización, Se requieren planear las acciones necesarias durante el período en que la infraestructura de TI se encuentra inactiva y en proceso de recuperación y reanudación de los servicios para priorizar cuales actividades y servicios deben entrar en operación inmediatamente dentro de la entidad.

Finalmente, es necesario tener en cuenta que los responsables del negocio deben conocer la importancia de tener una inversión de TI planeada que permita innovar tecnológicamente y que responda adecuadamente a los problemas generados por la interrupción de los servicios y permita que las empresas puedan aplicar exitosamente los criterios de recuperación y reanudación de las operaciones del negocio.

- ✓ **Objetivo General**

Disponer de un documento guía por medio del cual INFITULUA EICE puedan consultar los lineamientos de seguridad ante situaciones de emergencia a fin de mitigar el impacto producido por la interrupción de los servicios de alta criticidad que afectan sensiblemente las operaciones del negocio.

El Plan de continuidad del negocio, se conforma de un conjunto de directrices y procedimientos plasmados en un documento técnico, para que cada entidad pueda tomar las acciones pertinentes con miras a la recuperación y restablecimiento de los servicios e infraestructuras de TI interrumpidas por situaciones de desastre o emergencias ocurridas en cualquier instante dentro de las organizaciones.

El análisis de impacto del negocio como parte del plan de continuidad del negocio, debe entenderse como un marco conceptual sobre el cual las entidades deben planear integralmente los alcances y objetivos, que permiten proteger la información, en todas sus áreas críticas.

Las entidades deben establecer un análisis de impacto del negocio, que este alineado con el Plan General de Continuidad del Negocio de la Entidad; este debe tener una estrategia de continuidad de TI, que contenga los objetivos globales de la entidad, con respecto a las dimensiones de disponibilidad de datos, infraestructura tecnológica y recurso humano.

Para desarrollar el plan de continuidad del negocio de TI se debe tener en cuenta:

- ✓ Diseñar una estrategia de continuidad de los servicios de TI, que tenga como base la reducción del impacto de una interrupción en los servicios críticos de TI del negocio, este debe estar difundido, aprobado y respaldado por los directivos de la entidad.
- ✓ Realizar un análisis e identificación de recursos críticos de TI vitales, de esta manera se establece una estrategia que genere prioridades en caso de presentarse una o varias situaciones que causen interrupciones.

- ✓ Establecer procedimientos de control de cambio, que permita asegurar que el plan de continuidad de TI, se encuentre actualizado y permita afrontar las amenazas que traen consigo las nuevas tendencias tecnológicas sin perder el alcance de los requerimientos de la Entidad.

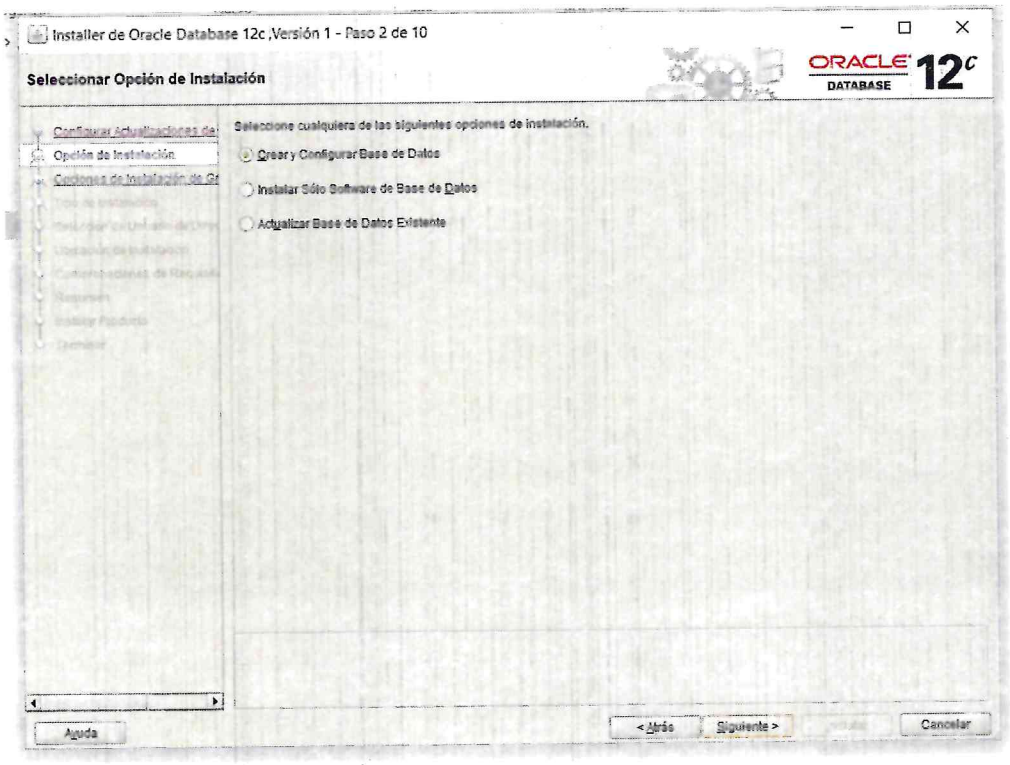
- ✓ Elaborar un plan de pruebas de continuidad de TI, que permita verificar y asegurar que los sistemas de TI, puedan ser recuperados de forma segura y efectiva, atendiendo y corrigiendo errores, que atenten contra la disponibilidad de las operaciones.

- ✓ Realizar capacitaciones del plan de continuidad de TI y análisis de impacto del negocio, a los entes o partes involucradas de la organización (Equipo de seguridad de sistemas de información de la entidad), para que conozcan cuáles son sus roles y responsabilidades en caso de incidentes o desastres. Es necesario verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia generadas dentro de la entidad.

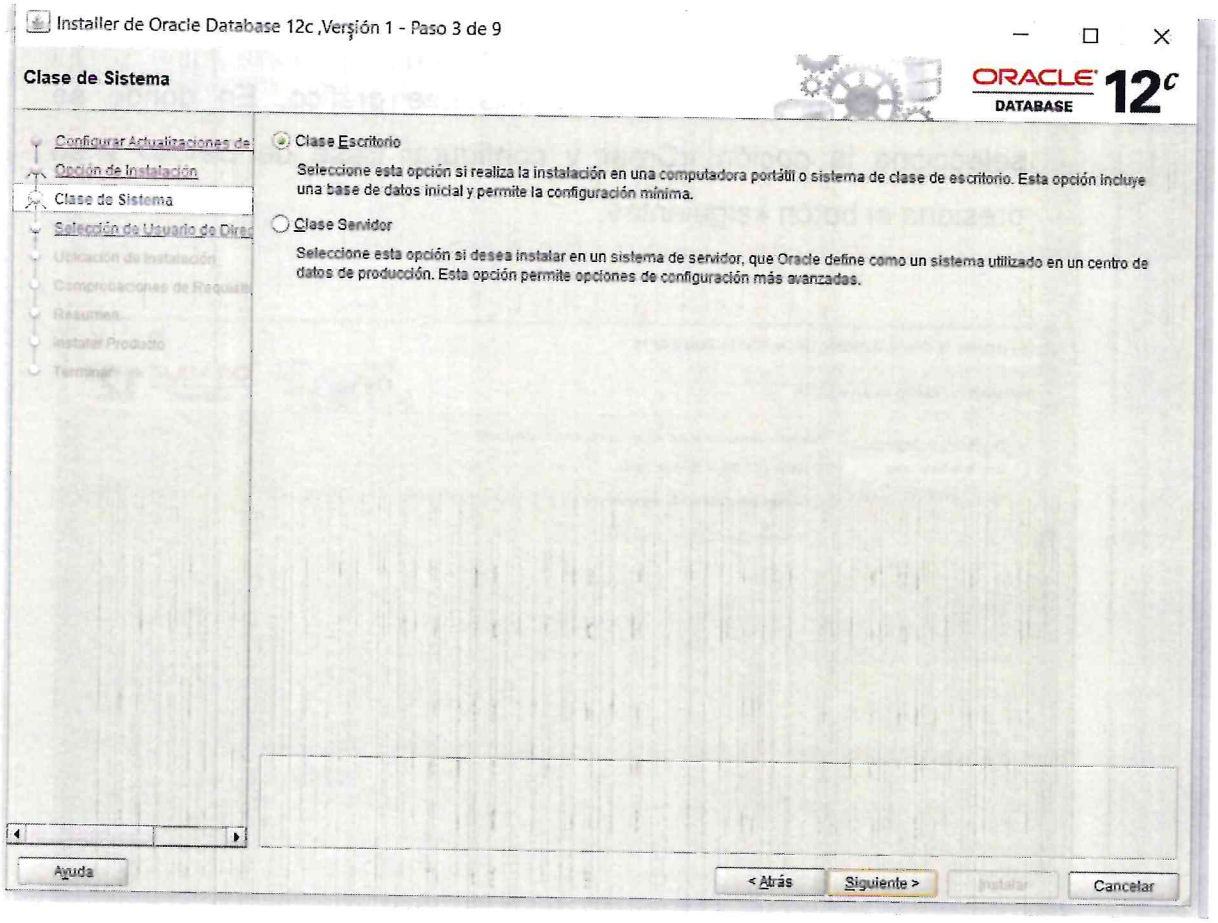
- ✓ Tanto el plan de continuidad de TI como el análisis de impacto del negocio deben estar disponibles apropiadamente dentro de la organización y en manos de los responsables de las áreas de TI quienes de forma segura deben garantizar su aplicabilidad en los momentos críticos, a su vez la entidad debe propender por un plan de sensibilización al interior de la misma con el propósito de indicar a todos sus miembros sobre la importancia de contar con un plan de continuidad y de análisis del negocio que van a garantizar el normal funcionamiento de las operaciones regulares en caso de presentarse problemas críticos en los sistemas de información y comunicaciones de la entidad.

- ✓ **Creación Bases de Datos Contenedoras.**

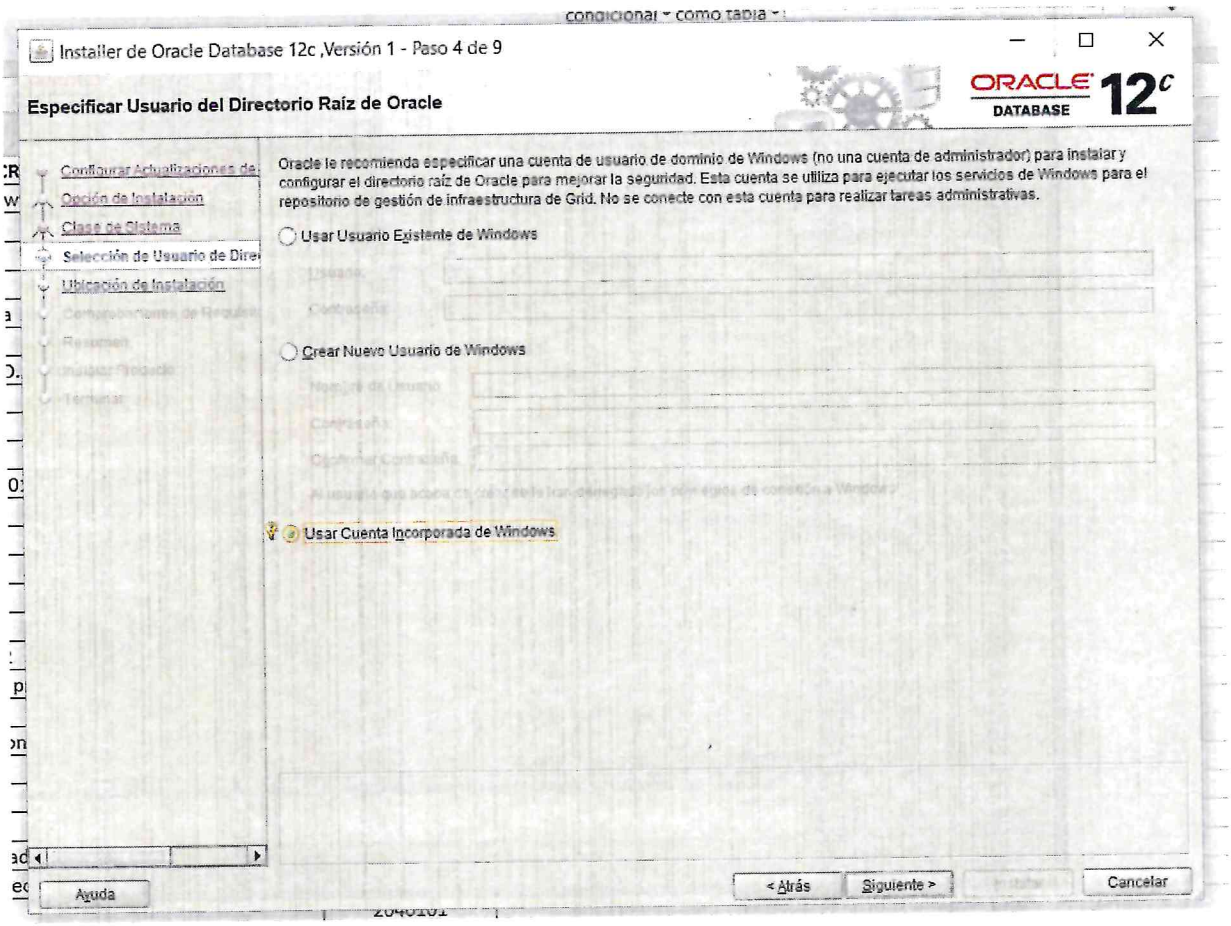
- ✓ Ejecutar el instalador de la base de datos.
- ✓ Posteriormente, se muestra el asistente gráfico. En donde se selecciona la opción «Crear y configurar Base de Datos» y se presiona el botón «siguiente».



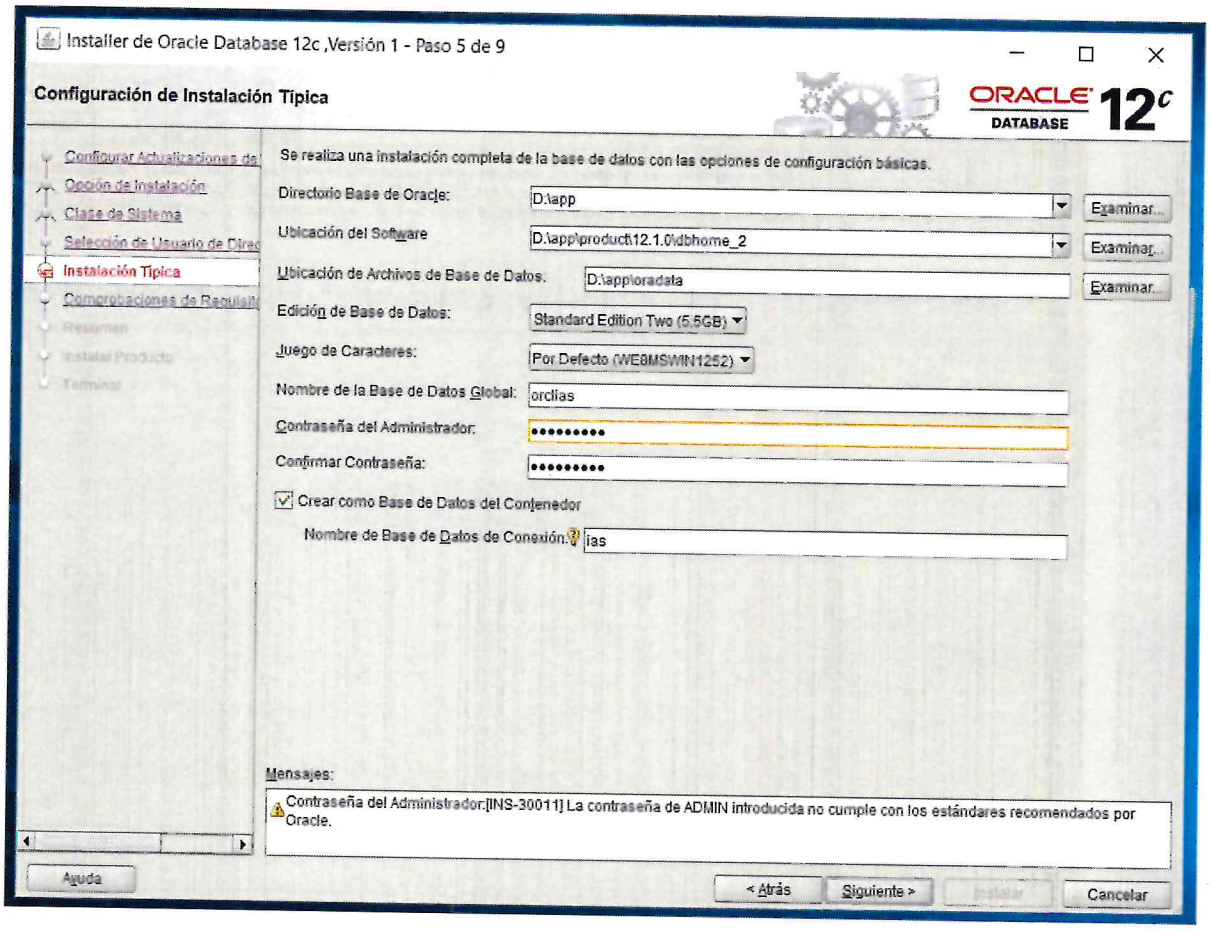
Elegimos la opción <<CLASE ESCRITORIO>>



Elegimos la opción <<USAR CUENTA INCORPORADA DE WINDOWS>>



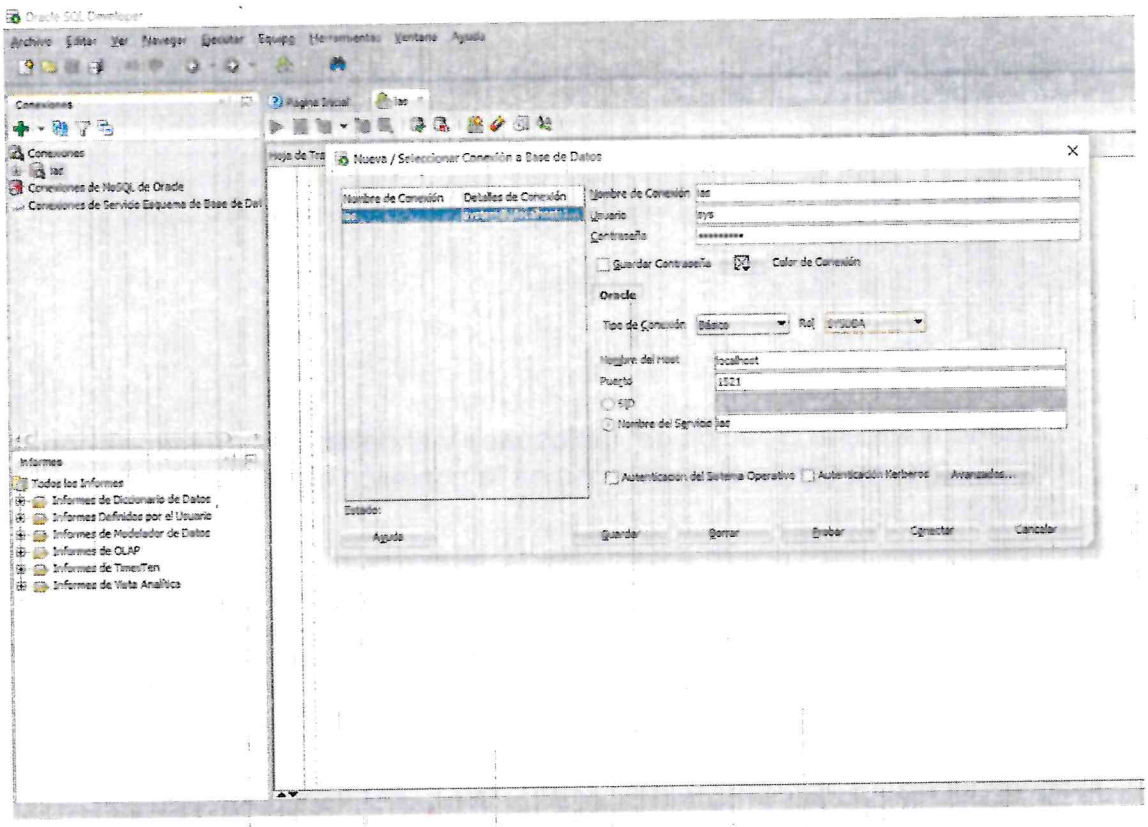
Se procede a configurar la base de datos eligiendo la ubicación donde se instalará y el nombre que tendrá la base de datos global y la de conexión.



Dar click en <<SIGUIENTE> hasta que comience la instalación.

Terminada la instalación procedemos a ejecutar SQL DEVELOPER para gestionar la conexión con la base de datos.

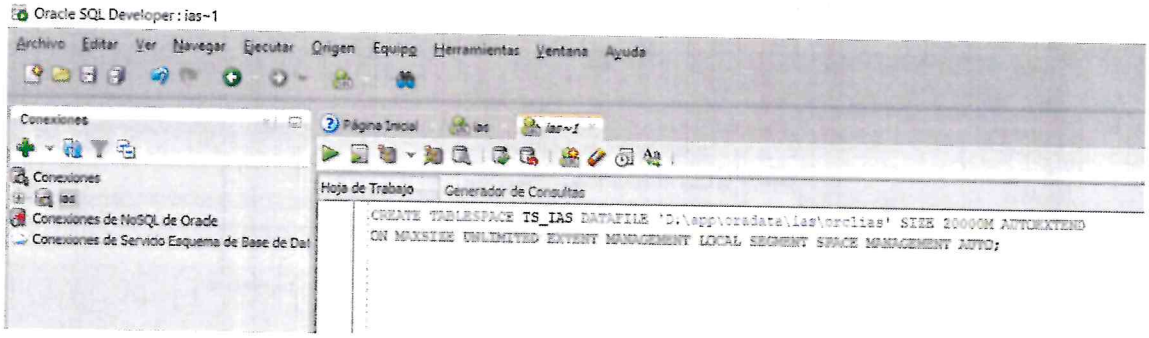
Agregamos la conexión en el sql developer dándole el nombre de la base de datos de conexión y utilizando el usuario sys.



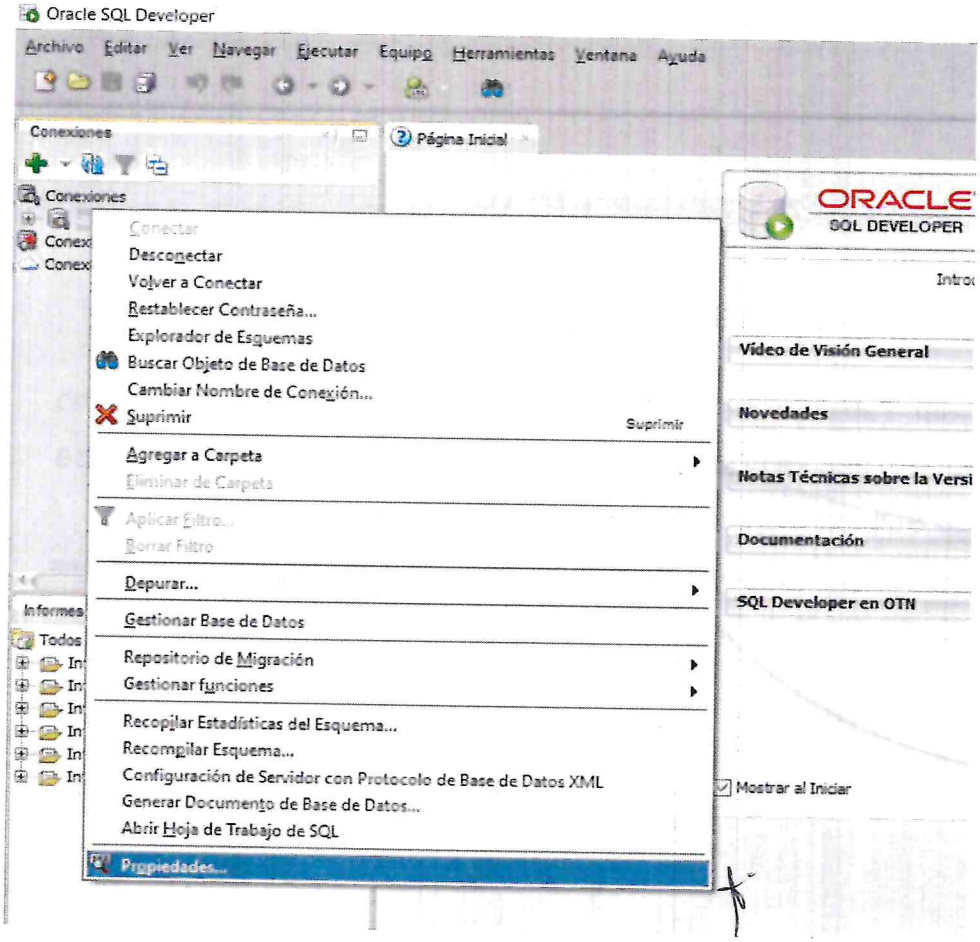
✓ **Creación de TABLESPACE y DATAFILE.**

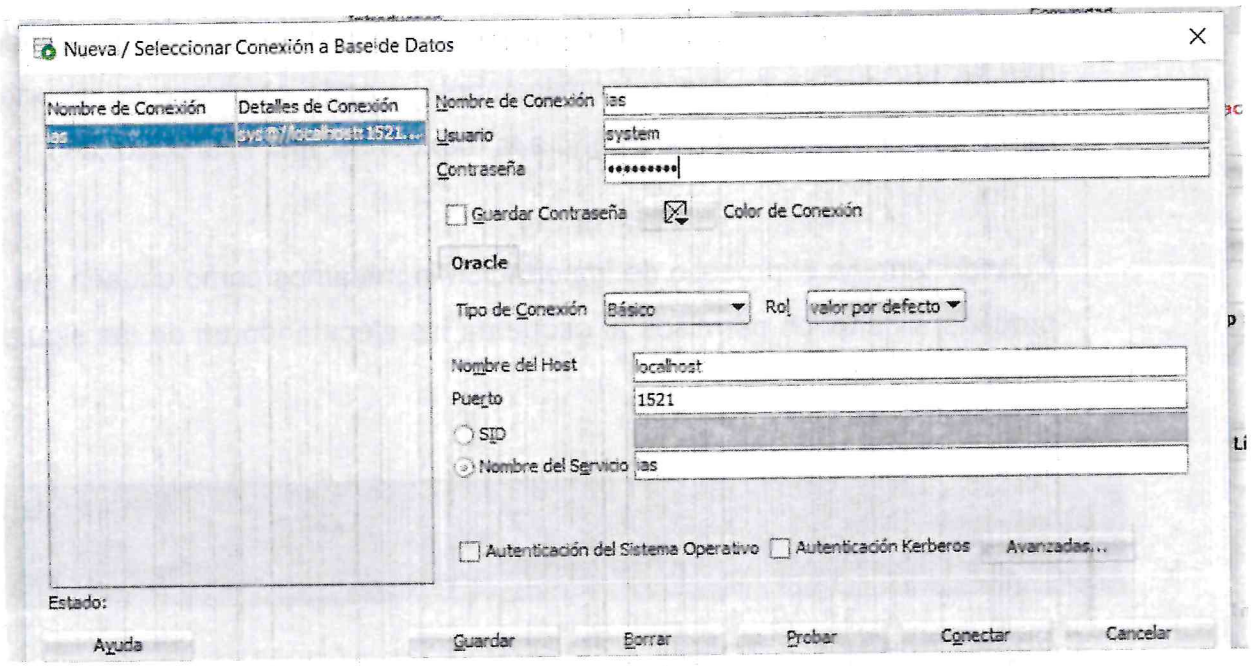
Para crear Tablespaces y Datafiles se debe conectar por SQL como SYSDBA a la cdb en la cual se desean crear. Posteriormente se ingresa el código SQL correspondiente a la acción deseada.

- Para crear un Tablespace con un Datafile se utilizan las siguientes líneas.

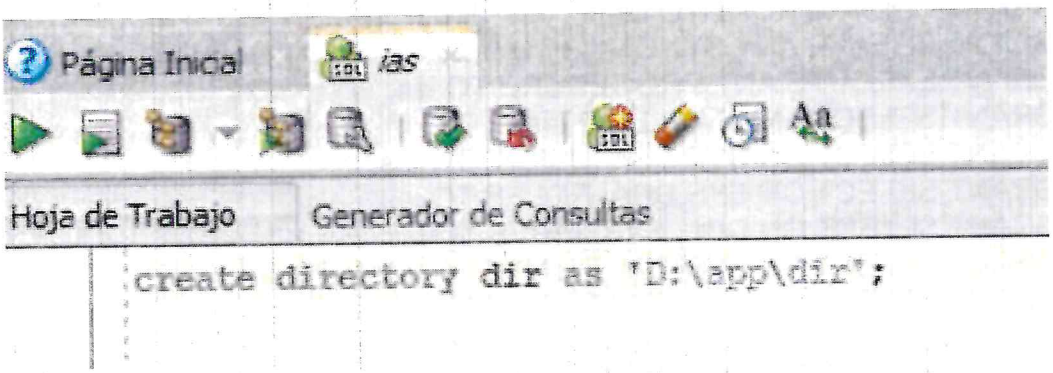


Cuando finalice la creación del tablespace y el datafile ingresamos con el usuario system dando click derecho en la conexión que tenemos en sql developer.





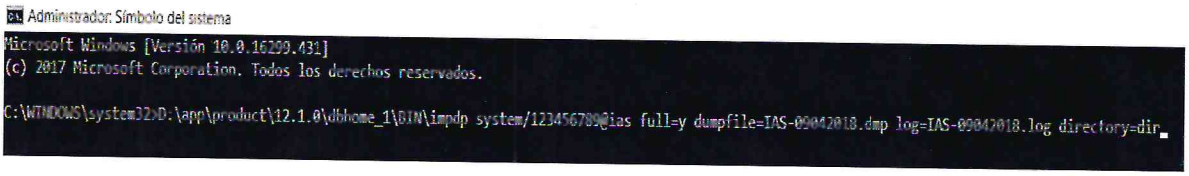
se procede a crear el directorio donde estará el archivo .dmp que se importará a la base de datos



Una vez creado el directorio ejecutamos la consola de comandos CMD para hacer la importación con la siguiente línea.

D:\app\product\12.1.0\dbhome_1\BIN\impd system/contraseña del usuario system full=y dumpfile=nombre del archivo.dmp log=nombre que tendrá el archivo log que se creara automáticamente cuando comience la importación directory= nombre que se le asigno a la ruta donde está el archivo.dmp

Cuando termina el proceso de importación ingresamos como usuario sys y se procede a darle los permisos al esquema ias ejecutando un de las siguientes líneas.

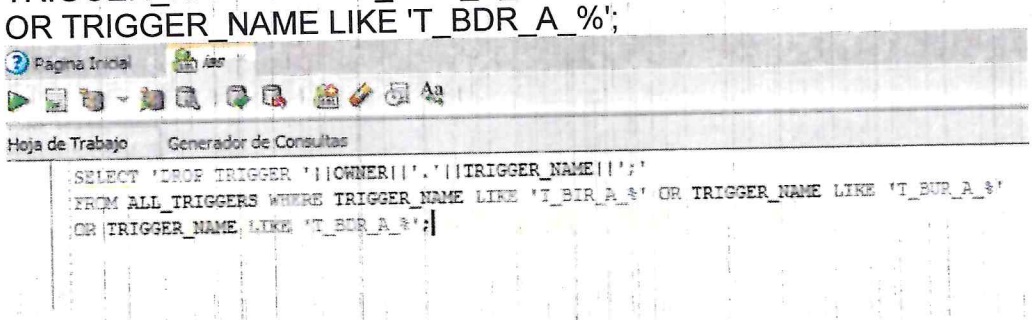



```
GRANT CONNECT  TO ias;
GRANT RESOURCE TO ias;
GRANT GRANT ANY ROLE TO ias;
GRANT GRANT ANY PRIVILEGE TO ias;
GRANT CREATE USER TO ias;
GRANT CREATE ROLE TO ias;
GRANT CREATE ANY SYNONYM TO ias;
GRANT EXECUTE ANY PROCEDURE TO ias;
GRANT SELECT ANY TABLE TO ias;
GRANT SELECT ON SYS.DBA_USERS TO ias;
GRANT SELECT ON SYS.DBA_ROLES TO ias;
GRANT SELECT ON DBA_SYS_PRIVS TO ias;
GRANT SELECT ON SYSTEM_PRIVILEGE_MAP TO ias;
GRANT SELECT ON DBA_ROLE_PRIVS TO ias;
GRANT SELECT ON ALL_OBJECTS TO ias;
GRANT SELECT ON ALL_SYNONYMS TO ias;
GRANT SELECT ON DBA_TS_QUOTAS TO ias;
GRANT SELECT ON DBA_JOBS TO ias;
GRANT SELECT ANY TABLE TO ias;
GRANT CREATE ANY TRIGGER TO ias;
GRANT CREATE TRIGGER TO ias;
GRANT DROP ANY TRIGGER TO ias;
GRANT ALTER PROFILE TO ias;
```

```
GRANT CREATE PROFILE TO ias;
GRANT DROP PROFILE TO ias;
GRANT ALTER ANY PROCEDURE TO ias;
GRANT CREATE ANY PROCEDURE TO ias;
GRANT CREATE PROCEDURE TO ias;
GRANT DROP ANY PROCEDURE TO ias;
GRANT ALTER USER TO ias;
GRANT BECOME USER TO ias;
GRANT DROP USER TO ias;
GRANT DBA TO ias;
GRANT ALTER ANY TRIGGER TO ias;
GRANT SELECT ON V_$SESSION TO ias;
GRANT SELECT ON V_$PARAMETER TO ias;
GRANT EXECUTE ON DBMS_PIPE TO ias;
GRANT AUDISOLU_ADMIN TO ias;
GRANT AUDISOLU_USER TO ias;
GRANT CREATE PUBLIC SYNONYM TO ias;
GRANT CREATE SYNONYM TO ias;
GRANT DROP ANY SYNONYM TO ias;
GRANT DROP PUBLIC SYNONYM TO ias;
GRANT SELECT ON user$ TO IAS;
```

Ingresando con el usuario system ejecutamos la siguiente línea.

```
SELECT 'DROP TRIGGER '||OWNER||'.'||TRIGGER_NAME||';'
FROM ALL_TRIGGERS WHERE TRIGGER_NAME LIKE 'T_BIR_A_%' OR
TRIGGER_NAME LIKE 'T_BUR_A_%'
OR TRIGGER_NAME LIKE 'T_BDR_A_%';
```

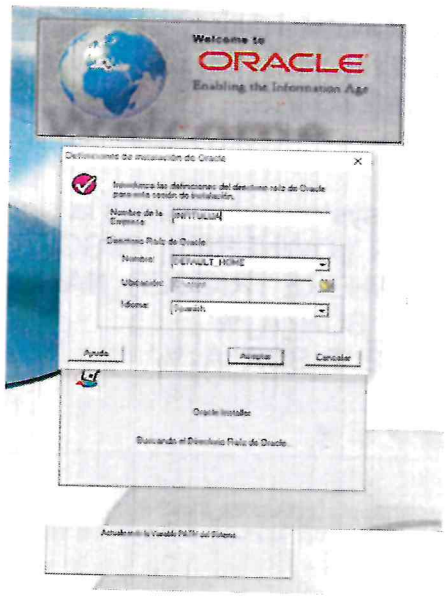


Con esto nos cargara un listado de trigger que debemos eliminar seleccionando todas las líneas que se muestran cuando se ejecuta la sentencia SQL.

Después de haber eliminado los trigger tenemos lista la base de datos para ser utilizada.

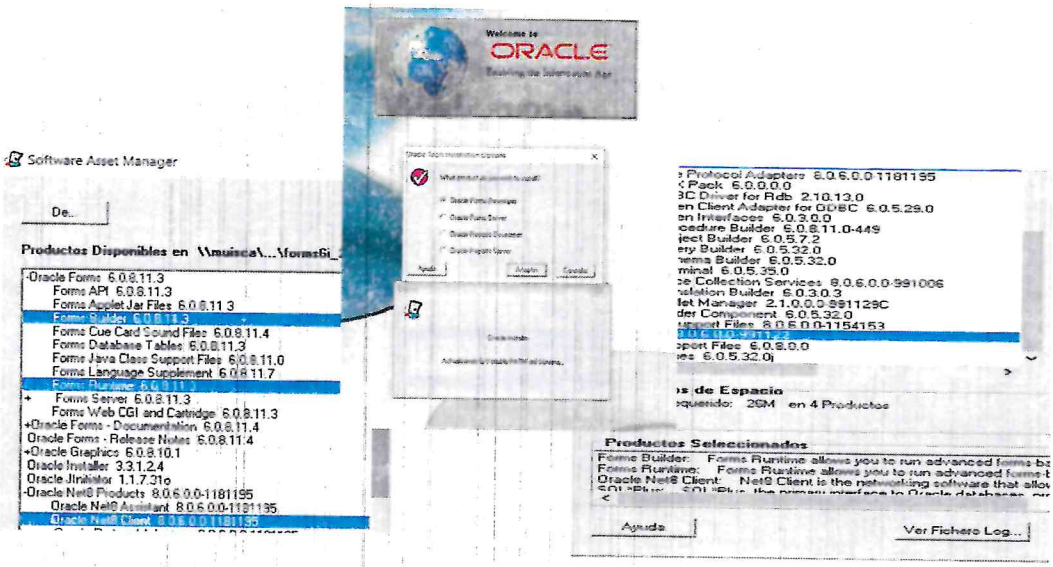
INSTALACION DE IAS SOLUTION

1.EJECUTAR EL INSTALADOR UBICADO EN EL SERVIDOR
I:\solution\Forms6i_2_instalador_principal
INGRESAR EL NOMBRE DE LA EMPRESA <<ACEPTAR>>



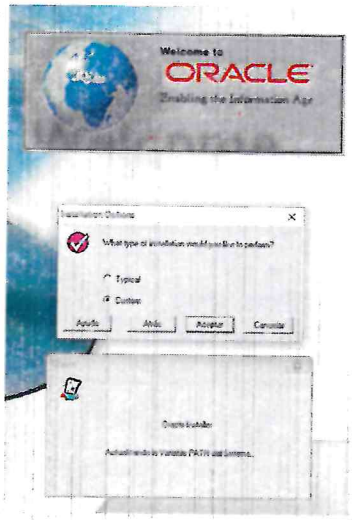
2.Elegir la opción Oracle forms developer <<ACEPTAR>>

Elegir la opción custom <<ACEPTAR>>



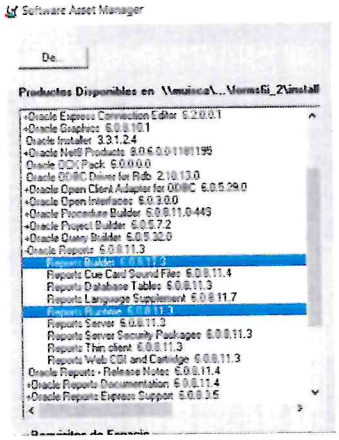
3.Elegir las opciones tal cual se muestra en la imagen luego dar click <<INSTALAR>>

Cuando termine la instalación dar click en salir y ejecutar de nuevo el instalador.

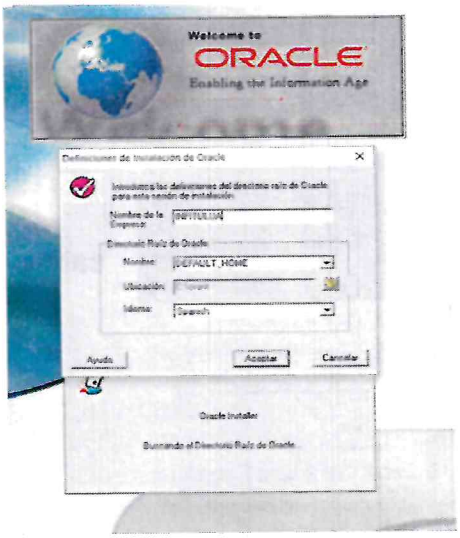


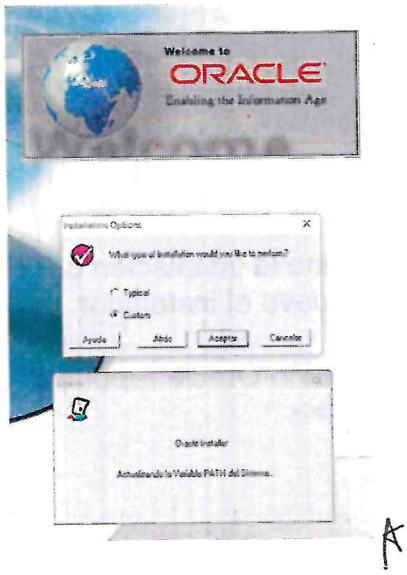
4.Elegir la opción Oracle reports developer <<ACEPTAR>>

5.Elegir las opciones que se muestran en la imagen y dar click <<INSTALAR>>

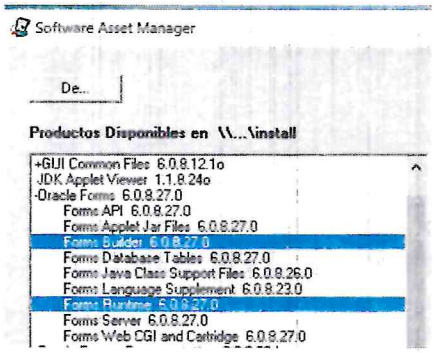


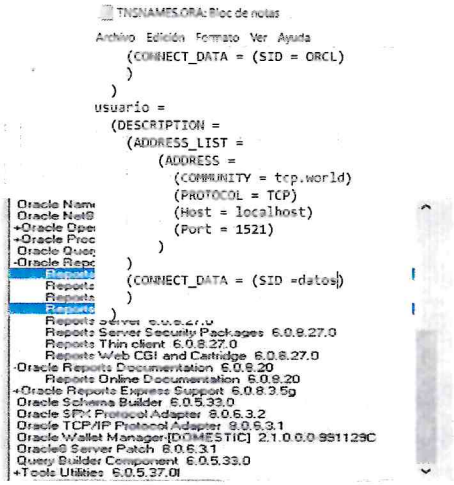
6.Cuando termine la instalación salir del instalador y ejecutar el parche que tendrá una interfaz igual al instalador. I:\solution\forms_patch_18_p4948577_600_WINNT



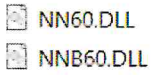


7. Seleccionar la opciones que se muestran en la imagen y dar click <<INSTALAR>>.

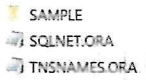




8.Una vez instalado el cliente se procede a copiar los dll (I:\solution\parche reports) a la siguiente ubicación "C:\orant\BIN" en el PC donde se instaló IAS.



9. Copiar el archivo TNSNAMES.ORA del servidor (I:\solution) y pegarlo en "C:\orant\NET80\ADMIN" editar el TNSNAMES.ORA para gestionar la conexión del cliente con la base de datos.



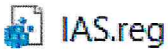
-Agregar las siguientes líneas en tnsnames.

NOMBRE DEL EQUIPO =
(DESCRIPTION =
(ADDRESS_LIST =

```
      (ADDRESS =
        (COMMUNITY = tcp.world)
        (PROTOCOL = TCP)
        (Host =localhost o la dirección ip )
        (Port = 1521)
      )
    )
    (CONNECT_DATA = (SID = NOMBRE DE LA BASE DE DATOS)
    )
  )
```

10. Por último ejecutar el registro. Acceder al servidor I:\solution\ACCESO y copiar el archivo (IAS_64.reg) y pegarlo al escritorio del PC local y ejecutarlo

11. Copiar el icono IAS de la ruta: I:\solution\ACCESO y pegarlo en el escritorio del PC local para ejecutar el aplicativo.



El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de

Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

A nivel metodológico es importante tener presente que el (MSPI) cuenta con una serie de guías anexas que ayudarán a las entidades a cumplir lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo, buscando a su vez comprender cuáles son los resultados a obtener y como desarrollarlos, incluyendo los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

b. INFITULUA EICE solo tiene servicios de copias de seguridad en la nube.

✓ **Definición de Cloud Computing**

Cloud Computing es un modelo que proporciona acceso a unos recursos de computación configurable. Por ejemplo redes, servidores, almacenamiento, aplicaciones y servicios. "Cloud computing" es un nuevo modelo de prestación de servicios de negocio y tecnología, que permite incluso al usuario acceder a un catálogo o, de forma flexible y adaptativa, en caso de demandas no previsibles o de picos de trabajo, pagando únicamente por el consumo

efectuado, o incluso gratuitamente en caso de proveedores que se financian mediante publicidad o de organizaciones sin ánimo de lucro."

El NIST define Cloud computing mediante la descripción de cinco características esenciales, tres modelos de servicio en Cloud y cuatro modelos de despliegue para Cloud.

- ✓ **Evidencia Digital**

DOCUMENTO TALLER QUE EN EL MOMENTO SE ENCUENTRA EN ACTUALIZACIÓN

- ✓ **Plan de Comunicación Sensibilización y Capacitación**

En la última década, las tecnologías de información y comunicaciones se han convertido en la herramienta por excelencia para la optimización de los procesos y el funcionamiento eficaz de una empresa.

Con el uso de la tecnología, surgen a su vez amenazas y vulnerabilidades asociadas, que pueden llegar a afectar la disponibilidad, privacidad e integridad de la información que se encuentra disponible en las diferentes plataformas, afectando de esta manera el desempeño normal de la Entidad.

Para esto, el modelo de seguridad y privacidad indica pautas específicas para guiar a las instituciones a robustecer sus plataformas y mitigar amenazas que pueden llegar a traer consigo las tecnologías implementadas, sin embargo, un programa robusto de seguridad y privacidad de la información no se basa únicamente en el aseguramiento de plataformas y procesos, sino que también debe involucrar los factores humanos, que en muchos casos, son la principal causa de los incidentes de seguridad dentro de un sistema determinado, esto debido a que no conocen sobre seguridad de la información y su rol dentro de una Entidad.

Muchas instituciones no prestan la suficiente atención a su recurso humano, que puede llegar a ser el eslabón más débil en la cadena de la seguridad de la información, por lo que es necesario sensibilizarlos o capacitarlos sobre la importancia de la preservación de la disponibilidad, integridad y confidencialidad de la información.

- ✓ **Objetivos**

Este documento tiene como objetivo establecer lineamientos para la construcción y mantenimiento del plan de capacitación, sensibilización y comunicación de la seguridad de la información, para así asegurar que este, cubra en su totalidad los funcionarios de la Entidad, asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información dentro de las entidades del Estado, se busca:

- Definir los temas para la capacitación en seguridad de la información, de acuerdo con el público objetivo.

- Establecer la metodología que les permita evidencias cuales son las necesidades de capacitación para la entidad.

- Construir materiales para sensibilización y entrenamiento.

- Evaluar, medir y cuantificar, si el programa implementado genera impacto en el desarrollo de las actividades de la Entidad.

- ✓ **Descripción General**

Un programa efectivo de sensibilización, capacitación y comunicación en seguridad de la información debe explicar de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas y la información, que generalmente están plasmadas en las políticas y procedimientos de seguridad

de la información que la Entidad, requiere que sean cumplidos por parte de todos los usuarios del sistema.

Cualquier incumplimiento a las políticas, debe llevar a la imposición de una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad correspondiente a su rol y responsabilidades dentro de la Entidad.

Teniendo en cuenta lo anterior, un plan de capacitación, sensibilización y comunicación adecuado, debe llevarse a cabo con base a las siguientes 4 fases:

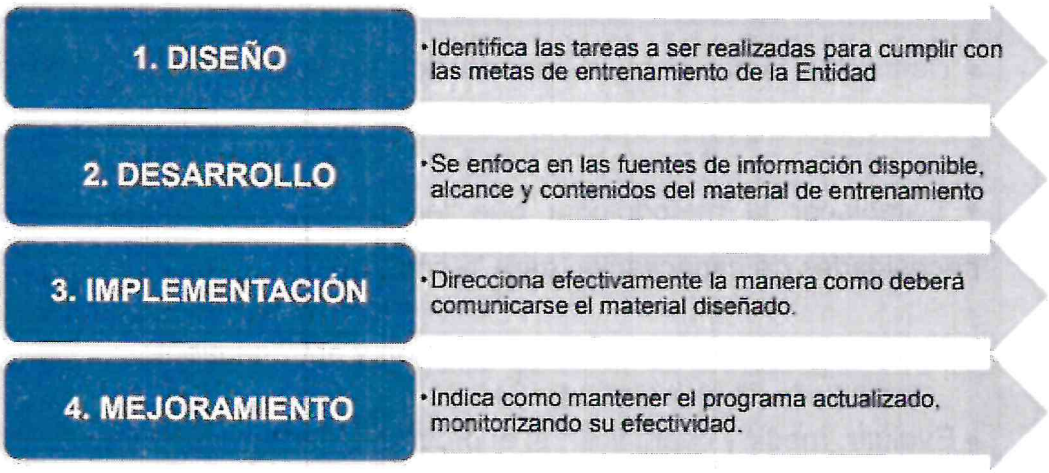


Figura 1. Fases plan de sensibilización, capacitación y comunicación

- ✓ **Identificación de Necesidades**

Para poder diseñar el plan apropiadamente, deben identificarse las necesidades dentro de la Entidad, el resultado de identificar estas necesidades, es la justificación que se tendrá para implementar el plan.

Es clave involucrar en el hallazgo de dichas necesidades a todo el personal, la siguiente clasificación de roles, podría ayudar a identificarlas en toda la Entidad y cada rol tendría diferentes objetivos especiales de conocimiento:

EJECUTIVOS	Deben conocer y entender las leyes y directivas que forman la base del programa de seguridad, también deben comprender el liderazgo que su rol tiene y que son el ejemplo a seguir de todas las demás unidades.
PERSONAL DE SEGURIDAD (OFICIALES DE SEGURIDAD)	Son los asesores expertos en seguridad, deben estar bien preparados en políticas de seguridad y buenas prácticas
DUEÑOS DE SISTEMAS	Deben entender bien las políticas de seguridad, así como también conocer sobre los controles de seguridad y la relación que tienen con los sistemas que manejan.
ADMINISTRADORES DE SISTEMAS Y PERSONAL DE SOPORTE	Estos funcionarios deben tener un buen nivel de preparación a nivel técnico de seguridad (implementación y prácticas de seguridad efectivas) para soportar las operaciones críticas del Entidad de manera apropiada.
USUARIOS FINALES	Requieren de un alto grado de sensibilización sobre la seguridad y las reglas de comportamiento adecuadas con los sistemas que tienen a disposición.

Tabla 1. Roles Y Necesidades En Capacitación Más Comunes

- ✓ **Definir Prioridades**

dichas prioridades pueden ser contempladas con base a los siguientes aspectos:

DISPONIBILIDAD DE RECURSOS/MATERIALES

- Si hay presupuesto disponible sin ningún problema, es posible iniciar con los aspectos más claves que se consideren, sin embargo, se debe contemplar tiempos de desarrollo de material y/o instructores.

IMPACTO EN LA ORGANIZACIÓN

- Dependiendo del rol o impacto de ciertos cargos en la organización, puede ser necesario dar prioridad a la capacitación o sensibilización a cierta población.

NECESIDADES CRITICAS DE PROYECTOS

- Por ejemplo, para poder, desplegar un nuevo sistema operativo, es necesario realizar una capacitación a todos los usuarios previo al despliegue.

ESTADO ACTUAL DEL PLAN (BRECHAS)

- Brechas o falencias que se hayan identificado en el plan y que se necesiten corregir.

Administración De Contraseñas	Uso Y Manejo De Inventario
Malware y sus diferentes tipos	Software Permitido/Prohibido En La Entidad
Políticas Organizacionales Relacionadas Con Seguridad De La Información	Uso De Dispositivos De La Entidad Fuera De Las Instalaciones
Uso De Correo Electrónico E Identificación De Correos Sospechosos	Seguridad En El Puesto De Trabajo
Uso Apropiado De Internet	Temas de control de acceso a los sistemas (privilegios, separación de roles)
Política De Escritorio Limpio	**Ingenieria Social**
Sanciones Por Incumplimiento De Las Políticas	**Gestión De Incidentes (Como reportar, que puedo reportar)**

Spam	"Shoulder Surfing"
Backups Y Recuperación	Cambios En Los Sistemas
Amenazas Y Vulnerabilidades Comunes	Roles Y Responsabilidades En La Entidad

✓ **Indicadores de un Plan de Capacitaciones Exitoso**

Un plan podría considerarse exitoso si se manejan o se tienen los siguientes aspectos:

1. Suficientes fondos para su desarrollo y mejoramiento.

2. Una estrategia bien enfocada en los diferentes roles de la Entidad.

3. Uso de MÉTRICAS, que permitan saber si el plan está funcionando bien. Por ejemplo (porcentaje de usuarios capacitados apropiadamente, porcentaje de ataques de ingeniería social exitosos se ha reducido, porcentaje de usuarios que hayan recibido material de sensibilización etc…).

4. La alta gerencia acata las normas de seguridad de la información y no utilizan su estatus para evadirlas, esto indica un cambio significativo en la cultura de la Entidad.

5. Reconocimientos a nivel estatal por gestión ejemplar.(Por ejemplo premios Excelencia de Gobierno En Línea).

6. Motivación por parte de los impulsores de los planes para mejorar cada vez más.

7. Aumento en el reporte de incidentes de seguridad de la información y mejora en la gestión de este proceso.

- ✓ **Recomendaciones Generales**

• El usuario final es clave para el desarrollo de un programa de gestión de la seguridad de la información, sin un usuario sensibilizado acerca de las amenazas y vulnerabilidades a los que está expuesto, es más probable que se produzcan incidentes de seguridad que puedan a tener impacto considerable dentro de la Entidad.

- Un personal con entrenamiento adecuado, es un personal que puede responder más rápidamente a algún incidente de seguridad, que puede ayudar a contener y evadir eventos negativos de una manera más óptima y por consiguiente ayuda a disminuir los riesgos.

- La sensibilización se centra en modificar el comportamiento de las personas, mientras que el entrenamiento se basa en enseñar a realizar alguna labor específica.

- El apoyo y compromiso de la alta dirección es clave para poder llevar a cabo un buen plan de capacitación.

- Las métricas son fundamentales para el mejoramiento continuo de cualquier proceso de gestión de seguridad incluyendo el de capacitación y sensibilización.

- El desarrollo de material para sensibilización es en mayor medida más sencillo de desarrollar que un material de entrenamiento, en ocasiones es más fácil contratar a un tercero para este fin, generalmente a los proveedores de las plataformas se les solicita una fase de transferencia de conocimiento o de entrenamiento para que el personal de seguridad o de TI aprenda a realizar las labores necesarias con los dispositivos.

- ✓ **Auditoria**

La presente guía tiene como finalidad, indicar los procedimientos de Auditoria en el proceso de verificación de la implementación del modelo de seguridad y privacidad de la información.

A partir del entorno y el contexto determinado por la entidad, la auditoria es una fuente de mejora, permitiendo conocer las debilidades para generar fortalezas, a través de la comprobación, seguimiento y evaluación de la mejora continua.

Por lo tanto, se convierte en una herramienta sistemática, independiente, objetiva, documentada, práctica y medible sobre el cumplimiento de los objetivos de la entidad y es allí donde la mejora continua tiene un papel fundamental.

Las auditorias apoyan la toma de decisiones frente al nivel de implementación y complementa el ciclo de mejora continua en relación con el ciclo PHVA.

Se procura que las entidades tengan un enfoque de seguridad en el cual se incluya el desarrollo y mantenimiento de la misma, realizando mejoras en las áreas que se requiera.

Dependiendo de la entidad, dichos procedimientos pueden variar o si la entidad desea puede generar más procedimientos si lo considera conveniente.

- ✓ **Principios de Auditoria**

La base de la auditoria, recae en los principios que sirven como lineamiento en el desarrollo de la misma, la cual permite proporcionar resultados confiables, objetivos, pertinentes y suficientes para que la organización pueda tomar las decisiones acerca de lo avanzado.

A continuación, se describen cada uno de los principios:

Integridad: El profesionalismo del auditor se debe llevar a cabo a partir de su honestidad, imparcial, diligencia y responsabilidad, demostrando su competencia durante el ejercicio de la auditoria.

Presentación ecuánime: El resultado de la auditoria (hallazgos, conclusiones e informes) deben reflejar la veracidad y exactitud de la información que se presentó durante el desarrollo de la auditoria.

Debido cuidado profesional: La habilidad del auditor en formular los juicios de valor razonables durante toda la auditoria.

Confidencialidad: La seguridad de la información, durante el ejercicio de la auditoria. Es un factor importante sobre el uso y la protección de la información, garantizando que no se utilice de manera inapropiada.

Independencia: La actuación del auditor se refleja en la independencia, libre de sesgo y conflicto de intereses. La independencia es la base de la imparcialidad y la objetividad del resultado de la auditoria, es así como está se mantiene objetiva durante todo el proceso.

Enfoque basado en la evidencia: El proceso de auditoria es una actividad sistemática, la cual se basa en la toma de muestras de la información por el tiempo limitado que se establece para una auditoria. Toda muestra debe permitir verificar la fiabilidad de la auditoria.

- ✓ **Fases de la Auditoria**

En el marco de la auditoria, está cuenta con 3 fases relacionadas a continuación:

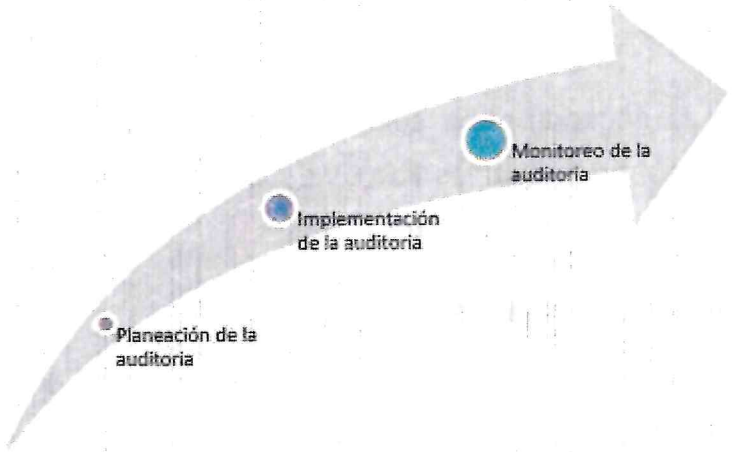


Imagen 1: Fases de la Auditoria

- ✓ **Planeación de la Auditoria**

Las auditorias se deben realizar al menos con una vez en el año, aunque esta periodicidad depende de las necesidades de la entidad. Durante la planeación se lleva a cabo el ciclo (planear) determinando los recursos, los procesos y el tiempo para llevar a cabo las auditorias, teniendo en cuenta como insumos las revisiones o seguimientos a la implementación del modelo de seguridad y privacidad de la información, observaciones por parte de la alta dirección, el desempeño de los procesos, los cambios en el entorno, controles internos, estrategias, entre otros.

Es importante que las auditorias se realicen con anterioridad a las auditorias de organismos de certificación y de control, con el fin de mejorar las deficiencias que pueda llegar a tener la implementación del modelo. También es necesario que los líderes de los procesos trabajen de forma alineada con el equipo de

seguridad o la Oficina de Control Interno o la dependencia que haga sus veces, para determinar mesas de trabajo orientadas a revisar su proceso de manera que el trabajo se realice proactivamente y no reactivamente. Con lo anterior los resultados pueden llegar a potencializar las acciones de mejora que agreguen valor a los procesos y por ende a la entidad.

La programación de la auditoria debe ser aprobada por la alta dirección y publicada en el sitio web, en la cual los líderes de los procesos conozcan las fechas y se preparen para recibir la auditoria.

- ✓ **Implementación de la Auditoria**

Durante esta fase, se prepara la auditoria. Inicia con la reunión de apertura, presentando la metodología, los tiempos y recursos que se utilizarán. Se recolecta y analiza la información evidenciando los hallazgos, las oportunidades de mejora y las fortalezas encontradas durante la auditoria. Una vez se culmine, se presenta durante la reunión de cierre las conclusiones de la auditoría.

- ✓ **Auditoria Informática**

Es la actividad de recolectar, consolidar y evaluar evidencia para comprobar si la entidad ha avanzado en la implementación de controles, protección de los activos, mantenimiento de la integridad de los datos, si tiene claro los objetivos de seguridad de la entidad y si utiliza bien los recursos. De este modo la auditoría informática mantiene y confirma la consecución de los objetivos tradicionales de la auditoría, que son:

- Protección de activos e integridad de datos.
- Gestión de protección de activos, de manera eficaz y eficiente.

La auditoría Informática, puede ser externa como interna y debe ser una actividad ajena a influencias propias de la entidad. La función auditora puede actuar de oficio, por iniciativa o por solicitud de la dirección de la entidad.

- ✓ **Auditoria de Sistemas**

La auditoría de sistemas, es aquella actividad donde se evalúa el manejo y la protección de la información residente en los sistemas de información, también califica la aptitud del recurso humano que gestiona estas plataformas y la eficiencia del recurso informático.
La función de la auditoria es preventiva, realiza revisiones utilizando recursos de hardware y software desarrollando procedimientos similares a los que emplea la entidad, con el fin de mejorar los procesos de la entidad.

El objetivo principal es la verificación del sistema de información, su confiabilidad y el uso del mismo por parte de la entidad.

- ✓ **Perfil del Auditor de Sistemas**

El Auditor es un asesor dentro de la entidad, su ubicación depende de la ubicación orgánica y funcional.

Se requieren calidades humanas, de gestor y de organizador, algunas de ellas:

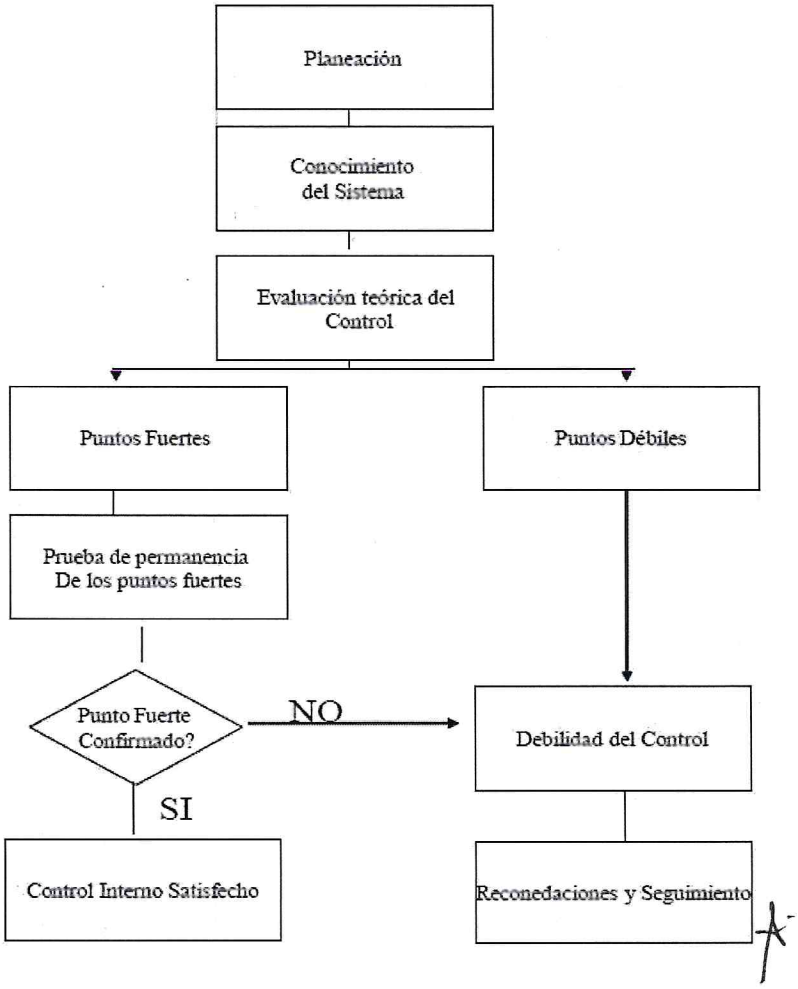
- Eficiencia en su misión en la entidad.
- Ser diplomático.
- Manejo de pedagogía.
- Conocimiento de herramientas y métodos, para llegar al objetivo a alcanzar.

- Conocimiento en técnicas de auditoria.

✓ **Metodología de la Auditoria en Sistemas**

La metodología inicia con un proceso de planeación, en esta se fijan los objetivos y las herramientas a usar, esto implica que hacer, como hacerlo y cuando hacerlo. Esta etapa incluye una investigación previa con el fin de conocer la operación de lo que se va a evaluar.

METODOLOGIA PARA AUDITORIA



- **TRANSICIÓN DE IPV4 A IPV6 PARA COLOMBIA**

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

En ese orden de ideas, este documento, presenta los lineamientos técnicos que se requieren tener en cuenta para seguir el proceso de transición de IPv4 a IPv6, en las distintas organizaciones del Estado, teniendo en cuenta su aplicación para todo el ciclo de desarrollo por fases que requiere el nuevo protocolo, en un ambiente controlado y seguro que permita consolidar una adopción del protocolo IPv6 con éxito en el país.

Para abordar esta temática se empezará por comentar que desde hace más de tres décadas, las redes de telecomunicaciones han venido creciendo exponencialmente generando una mayor demanda de servicios y oportunidades en la red mundial de internet; con el aumento de las tecnologías computacionales y de comunicaciones, ha aumentado el proceso de innovación tecnológica en los diversos dispositivos tanto alámbricos como inalámbricos, como por ejemplo, celulares, puntos de acceso, tabletas, servidores, equipos de almacenamiento entre otros, que comenzaron a incrementar la conectividad en muchas redes en el mundo y para ello han tenido que hacerlo con direcciones de internet que permiten establecer conexiones para cada elementos conectado a la red, estas direcciones se conocen como direcciones IP (Internet Protocol Versión 4), que en estos momentos entraron a una fase de agotamiento final, así mismo en el año 1992 la Internet Engineering Task Force IETF1 a partir de diversos grupos de trabajo definió el RFC 2460 (Especificaciones del Protocolo Internet Versión 6 (IPv6) que dio origen al

nuevo protocolo de conectividad denominado IPv6 o Ipng (Next Generation Internet Protocol).

En ese orden de ideas el protocolo IPv6, hace posible que todos los dispositivos tecnológicos usados para la conexión a internet, tengan una dirección en IPv6, la cual facilitará la conectividad en banda ancha, ofreciendo mejores servicios poniéndolos al alcance de toda la población a fin de estimular y ofrecer mejores oportunidades para el desarrollo mundial.

Así mismo, para cumplir con los objetivos de innovación tecnológica que exige el país, las entidades del país deben entrar en el proceso de transición del protocolo IPv4 hacia el nuevo protocolo IPv6 siguiendo las instrucciones descritas en la Circular 002 del 6 de julio de 2011 del Ministerio de Tecnologías de la Información y las Comunicaciones, que busca promover la adopción de IPv6 en Colombia.

Para entrar en el proceso de adopción de este nuevo protocolo, se recomienda realizar un inventario de los activos de información, revisar su actual infraestructura de computación y de comunicaciones, validar todos los componentes de hardware y software de que se disponga, revisar los servicios que se prestan, los sistemas de información, revisión de estándares y políticas para conocer el impacto de adopción de la nueva versión del protocolo IP, a fin de facilitar las labores de planeación e implementación de IPv4 a IPv6, garantizando que las operaciones continúen funcionando normalmente dentro de las entidades del estado.

Así mismo, para atender esta necesidad inminente de innovación tecnológica en el país, el Mintic, mediante este instrumento, desea proyectar los lineamientos necesarios para diagnosticar, sensibilizar, desarrollar e implementar el protocolo IPv6 en las entidades del estado, con el propósito de

adoptar el nuevo esquema de funcionamiento de manera paralela con el actual protocolo IPv4, de conformidad con la Circular 002 de Julio de 2011, garantizando que las infraestructuras de hardware, software y servicios continúen operando normalmente en las distintas instituciones del país.

Finalmente, el mismo documento, será el apoyo al plan guía de acompañamiento, que facilitará las acciones necesarias para la adopción del nuevo protocolo en las entidades del país, partiendo de la fase inicial de diagnóstico de las infraestructuras de TI (Hardware y el Software), hasta la fase final que contemple la implementación y el monitoreo del nuevo protocolo en las distintas instituciones.

- ✓ **Objetivos Específicos**

Presentar un marco de referencia para facilitar el proceso de transición de IPv4 a IPv6, que permita orientar a las Entidades del Gobierno y a la sociedad en general, en el análisis, la planeación, la implementación y las pruebas de funcionalidad del protocolo IPv6, con el fin de incentivar el proceso de adopción y despliegue del protocolo IPv6 en el país.

- ✓ **Beneficios de la Transición**

Los siguientes puntos son los beneficios que representa un proceso de transición de IPv4 a IPv6 que son importantes tener presente al momento de adoptar el nuevo protocolo con éxito, ellos son:

• La posibilidad de tener un mayor número de equipos conectados a la red de las entidades al ser implementada esta solución.

• Proceso técnicamente transparente para los usuarios de la red de comunicaciones y sus distintos servicios dentro de las organizaciones.

• La posibilidad de incrementar la movilidad de los usuarios al tener un número mayor de direcciones IP para la conectividad.

• Mejora de la seguridad a nivel de direccionamiento IP de la red en virtud de la arquitectura del nuevo protocolo y sus servicios.

• Reducción de los costos al implementar la solución de IPv6, en este sentido los costos podrían ser mayores de no implementarse el nuevo protocolo en las entidades.

• Se facilitará la aparición de nuevas aplicaciones y servicios sobre una gran variedad de plataformas.

• Gran número de direcciones IP para conexiones a Internet con el mundo exterior, facilitando el crecimiento de nuevas tecnologías como el internet de las cosas, las ciudades inteligentes, redes de sensores, entre otras.

• Los Proveedores de Servicio de Internet, tendrán que preparar el proceso de transición de IPv6, mediante la creación de un backbone nativo de IPv6 que apoye a los clientes en el enrutamiento de las nuevas direcciones IPv6 a fin de garantizar la publicación de servicios y aplicaciones que se consideren pertinentes hacia internet para todas las entidades del Gobierno.

• Para el ciudadano en general, la implementación de IPv6 será un proceso gradual cuya responsabilidad no será del gobierno, sino del proveedor del servicio de internet directamente y no deberá generar costos directos.

- ✓ **Planeación del Ipv6**

La fase de planeación representa una etapa crítica e importante del proceso de transición por cuanto comienza con el inventario de activos de información y se consolida con el plan de diagnóstico de las infraestructuras de TI de las

Entidades; para ello se recomienda tener en cuenta el modelo de referencia para la adopción de IPv6.

Las siguientes son las actividades a tener en cuenta en esta fase:

• Elaborar y validar el inventario de activos de información de servicios tecnológicos de las entidades y su interrelación entre ellos. Para esta actividad se requiere tener preparado el inventario de hardware y software, identificando claramente cuáles elementos (equipos y software) soportan IPv6, cuales requieren actualizarse y/o no soportan el nuevo protocolo, dejando la respectiva documentación en constancia al momento de optar hacia IPv6.

Para esta etapa se recomienda que para cada elemento del inventario de activos de información se pueda constatar con los fabricantes, y con los terceros si ha lugar, el cumplimiento de IPv6, a través de la certificación que avale el soporte del nuevo protocolo en las infraestructuras de TI.

• Analizar, diseñar, desarrollar y afinar el plan de diagnóstico de IPv6 en la red de las entidades del estado con base en lo establecido en el inventario de activos de información.

• Para la construcción del plan de diagnóstico, que es el pilar fundamental de esta fase I, se requiere la realización de la validación previa de la infraestructura tecnológica que permita medir el grado de avance en la adopción del protocolo IPv6 en las Entidades; dentro de dicha validación es necesario revisar el grado de compatibilidad del protocolo IPv6 con la infraestructura de TI las entidades de tal manera que la información recogida de esta tarea sea insumo para el inicio de la fase II de IPv6.

• Identificar la topología actual de la red y su funcionamiento dentro de la organización y con base en esto, proponer el nuevo diseño de red sobre IPv6.

• Generar el plan detallado del proceso de transición de esta fase hacia IPv6 con base en el plan de diagnóstico y el diseño de la red de comunicaciones, mencionados en los anteriores puntos.

• Planear el proceso de transición de los siguientes servicios tecnológicos: Servicio de Resolución de Nombres (DNS), Servicio de Asignación Dinámica de Direcciones IP (DHCP), Directorio Activo, Servicios WEB, Servidores de Monitoreo, Validación del Servicio de Correo Electrónico (Local o en la nube), Validación del Servicio de la Central Telefónica, Sistemas Ininterrumpidos de Potencia, Servicio de Backups, Servicio de Comunicaciones Unificadas e Integración entre Sistemas de Información, Servicios de ambiente colaborativo; así mismo revisar los procedimientos de implementación de estos servicios y las aplicaciones identificadas en esta fase, con base en los estándares de la RFC3 de IPv6.

• Validar el estado actual de los sistemas de información, los sistemas de comunicaciones, los sistemas de almacenamiento y evaluar la interacción entre ellos cuando se adopte el protocolo IPv6.

• Dentro del proceso de diagnóstico presentar cuales equipos de computación y de comunicaciones soportan IPv6 (IPv6-ready o IPv6-web), cuales requieren actualizarse y cuáles no se pueden soportar IPv6.

• Identificar la configuración y todos los esquemas de seguridad de la red de comunicaciones y sistemas de información.

• Revisar las políticas de enrutamiento para IPv6 entre los segmentos de red internos, de tal manera que el tráfico IPv6 generado internamente este plenamente controlado a través de zonas desmilitarizadas desde el firewall respectivo de cada entidad, se recomienda en todo caso revisar los RFC correspondientes a políticas de enrutamiento y seguridad de IPv6.

• Establecer el protocolo de pruebas para la validación de aplicativos, equipos de comunicaciones, equipos de cómputo, plan de seguridad y coexistencia de los protocolos IPv4 e IPv6 por cada Entidad.

• La ejecución y configuración de las pruebas piloto de IPv6, se debe realizar bajo un proceso metódico que implique inicialmente la creación de una Red de Área Local Virtual (VLAN) de prueba sobre el Core de la red, que incluya diversos equipos y servicios de misión crítica que contemple entre otros, el análisis del comportamiento de software, el análisis del hardware en cada dispositivo, el análisis y comportamiento de estos en la red de comunicaciones, su comportamiento dentro de los aplicativos de la entidad, el análisis de cada servicio ofrecido y agregación de carga de tráfico sobre esta VLAN, teniendo en cuenta que las pruebas realizadas deben estar sujetas a las mejores prácticas y metodologías de transición a IPv6 conservando el criterio técnico de Doble Pila o Dual Stack. Una vez se tenga la certeza de que la VLAN de pruebas, ha soportado todo el proceso de pruebas de funcionalidad sobre un ambiente de tráfico en doble pila controlado; el siguiente paso es replicar esta VLAN sobre toda la red de la organización que garantice la implementación y el funcionamiento del nuevo protocolo en toda la infraestructura de la entidad.

• Preparar una zona controlada para realizar pruebas de funcionalidad del nuevo protocolo de comunicaciones IPv6, es importante aislar un segmento de red o crear un nuevo segmento de red, el cual debe permitir aceptar cambios y activaciones necesarias para confirmar la funcionalidad de IPv6 sin afectar el ambiente de producción de los usuarios.

• Establecer los acuerdos de confidencialidad que sean necesarios sobre el tratamiento de la información ante terceros al momento de ejecutar el plan de transición.

• Preparar a los funcionarios de las Áreas de TI, de conformidad con los planes de capacitación establecidos por cada entidad para el protocolo IPv6 y establecer la sensibilización a las personas de toda la organización a fin de dar a conocer el nivel de impacto en la implementación del nuevo protocolo, de conformidad con el siguiente modelo de referencia de adopción de IPv6.

• Las entidades deberán entrar en sincronización y operación con los ISP (Proveedores de Servicios de Internet) con el fin de definir las estrategias de enrutamiento de IPv6 nativo.

Gráfica 1. Modelo de Referencia para la Adopción de IPv6

Entregables de esta Fase

• Plan de trabajo para la adopción de IPv6 en toda la organización.

• Plan de diagnóstico que debe contener los siguientes componentes:

- ✓ Inventario de TI (Hardware y software) de cada Entidad diagnosticada.

- ✓ Informe de cumplimiento de IPv6 por cada elemento de hardware y software (Red de comunicaciones, sistemas de almacenamiento, sistemas de cómputo, aplicativos, bases de datos, sistemas de seguridad, entre otros)
- ✓ Recomendaciones para adquisición de elementos de comunicaciones, de cómputo y almacenamiento con el cumplimiento de IPv6
- ✓ Informe con el plan de direccionamiento en IPv6
- ✓ Plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6
- ✓ Informe de preparación (Readiness) de los sistemas de comunicaciones, bases de datos y aplicaciones (Que tan preparada se encuentra la entidad en tema de adopción de IPv6).
- ✓ Documento que define los lineamientos de implementación de IPv6 en concordancia con la política de seguridad de información y los controles de seguridad informática de las entidades.

• Plan de capacitación en IPv6 a los funcionarios de las Áreas de TI de las Entidades y plan de sensibilización al total de funcionarios de las Entidades.

Tabla de actividades de la Fase I – Planeación de IPv6 Se recomienda a las entidades tener en cuenta la siguiente tabla y diligenciar el tiempo en meses que le lleve desarrollar cada actividad:

Fase I	Actividades Generales	Tiempo en meses de la actividad
Diagnóstico de la Situación Actual	Construcción del plan de Diagnóstico	
	Inventario de TI (Hardware, Software)	
	Análisis de la nueva topología de la infraestructura actual y su funcionamiento	
	Protocolo de pruebas de validación de aplicativos, comunicaciones, plan de seguridad y coexistencia de los protocolos	
	Planeación de la transición de los servicios tecnológicos de la Entidad	
	Validación de estado actual de los sistemas de información, los sistemas de comunicaciones, las interfaces y revisión de los RFC correspondientes.	
	Identificación de esquemas de seguridad de la información y las comunicaciones	

Tabla 1. Actividades de la Fase I

En el Instituto no se puede pasar a fase II o Fase de Implementación, debido a que no se ha superado la fase I.

c. ASEGURAMIENTO DEL PROTOCOLO IPV6

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

En ese orden de ideas, este documento, presenta los lineamientos y políticas que se requieren tener en cuenta para la seguridad del protocolo IPv6, en las distintas infraestructuras de Tecnologías de la Información y las Comunicaciones que las Entidades del Estado, teniendo en cuenta su aplicación en todo el ciclo de desarrollo que sigue el nuevo protocolo, en un ambiente controlado y seguro que permita consolidar el proceso de adopción de IPv6 con seguridad y con un nivel de impacto altamente positivo para todas las organizaciones del país.

- ✓ **Objetivos Específicos**

Presentar un marco de referencia sobre lineamientos de seguridad en IPv6, que sea referente para abordar el plan de diagnóstico, plan de implementación y monitoreo del proceso de transición de IPv4 a IPv6 en cada una de las Entidades del Estado, para adoptar el protocolo IPv6 con base en las características de Confidencialidad, Integridad, Disponibilidad y Privacidad de la información; a fin de generar mecanismos de direccionamiento IP de acceso seguro y uso eficiente de las infraestructuras de información y comunicación de los diferentes organismos del Estado.

- ✓ **Características De Ipv6**

El Protocolo de comunicaciones IPv6 Internet Protocol Version 6, fue desarrollado por Steve Deering y Craig Mudge en el año 1994, y posteriormente fue adoptado por la IETF (Internet Engineering Task Force), adicionalmente IPv6 también es conocido como IPng (IP Next Generation). El nuevo protocolo tiene el propósito de reemplazar progresivamente el protocolo IPv4 actualmente en uso por la comunidad de Internet, en razón al limitado número de direccionamientos en IP que no hace posible su crecimiento en las redes y servicios; las características generales del nuevo protocolo son:

✓ Definido por la RFC (Request For Comments)2 2460 de 1998.

✓ Tamaño del paquete 128 bits.

✓ Encabezado de base simplificado y de extensión.

✓ Identificación de flujo de datos, mejor calidad de servicio (QoS).

✓ Direccionamiento en Anycast, Multicast y Unicast.

✓ Incorpora mecanismos de IPSec (IP Security) al protocolo, cuya seguridad está a nivel del núcleo del mismo; por lo tanto la carga de paquetes se cifra con IPSec.

✓ Fragmentación de origen y destino de ensamble de paquetes.

✓ Conectividad extremo a extremo.

✓ IPv6 ofrece mejoramiento de las capacidades de autenticación y privacidad de los datos que transmite porque los paquetes que proceden de un origen son los indicados en la cabecera de autenticación, mientras que en IPv4, los paquetes pueden venir de orígenes distintos a los indicados en la cabecera.

✓ Interacción con nodos vecinos a través del protocolo ICMP (Internet Control Message Protocol for IPv6).

✓ Mecanismos de seguridad avanzada sobre los datos transmitidos.

✓ Espacio de direccionamiento elevado de aproximadamente de 340 Sextillones, 340 trillones de direcciones por pulgada cuadrada, 670 mil billones de direcciones por metro cuadrado.

LINEAMIENTOS DE SEGURIDAD PARA Ipv6

✓ La fase de implementación del protocolo IPv6 debe ser estructurado con base en los esquemas de seguridad de información, sobre los cuales se tengan contempladas las políticas de confidencialidad, integridad y disponibilidad de las Entidades

✓ Se requiere definir un plan de marcha atrás (Plan de Contingencias) para el caso de presentarse inconvenientes de indisponibilidad de los servicios, que atenten contra la seguridad de la información y de las comunicaciones de las Entidades al momento de implementar el protocolo IPv6.

✓ En el proceso de transición hacia el nuevo protocolo, revisar la seguridad de información de las infraestructuras de TI, la seguridad de IPv6 y el nivel de impacto de servicios como el Directorio Activo, Sistemas de Nombres de Dominio - DNS, Correo Electrónico, Servicio de Protocolo de Configuración Dinámica de Host – DHCP (Definido en el RFC3315 para DHCPv6), Sistemas Proxy, Servicios de aplicaciones, Servicios Web y Sistemas de Gestión y Monitoreo.

✓ Se recomienda mantener la utilización de los mismos nombres de servicios utilizados sobre la red tanto para IPv4 como para IPv6, de tal manera que la resolución de nombres de dominio se de en forma transparente tanto para Ipv4 como en IPv6, se exceptúa de esta regla los ambientes de prueba que se realicen sobre IPv6.

✓ De la misma manear que ocurre con IPv4, en Ipv6 se recomienda no usar direcciones IPv6 literales en el desarrollo del software y en el uso de librerías.

✓ Generar la documentación necesaria que contemple los aspectos de seguridad del entorno en los sistemas de comunicaciones, sistemas de información y sistemas de almacenamiento, que surjan del desarrollo de la implementación de IPv6.

✓ La implementación de IPv6 puede generar riesgos de seguridad de información, que impactan en los servicios de las entidades y pueden acarrear problemas; con el objeto de poder detectar estos riesgos se requiere hacer un análisis detallado que permita encontrar posibles vulnerabilidades y en efecto bajo IPv6 es necesario hacer esta labor debido a que el protocolo se apoya en otros protocolos como IPSec, HTTP, TCP, UDP o SIP.

✓ Disponer para las infraestructuras de TI, de varias zonas lógicas configuradas en el firewall, que estén segmentadas para cada uno de los servicios disponibles en la Entidad, a fin de garantizar la máxima protección una vez la red de comunicaciones comience a generar tráfico en IPv6.

✓ Disponer del equipo humano idóneo necesario para verificar y monitorear los problemas de seguridad de información que surjan al momento de ejecutar las fases de implementación y pruebas de funcionalidad, cuya labor está bajo la responsabilidad del Director de Seguridad de la Información – CISO (Chief

Information Security Officer) o del que haga sus veces y del equipo de trabajo de seguridad de las Áreas de TI de cada Entidad.

✓ La verificación y el entendimiento de los componentes de seguridad diseñados para el protocolo IPv6 son claves para evaluar, monitorear y mejorar el desempeño de los servicios y aplicaciones bajo IPv6, cuando estos empiecen a generar tráfico en los canales de IPv6. En este sentido el documento sobre "Política para la adopción de IPv6 en Colombia, estructuración y definición de Cintel y Mintic del año 2012", dice:

"Se debe dar paso a la transición de IPv4 a IPv6 como una herramienta para mejorar las condiciones de seguridad nacional y la seguridad de la información. Siempre que la adopción de IPv6 facilita las tareas de monitoreo y refuerza los protocolos de seguridad nacional, dado que con IPv6 cada usuario, cada equipo, cada terminal móvil puede recibir, de forma estática, una dirección IP que lo identifica, lo cual hace posible establecer con certeza la ubicación y el origen de la comunicación y permite adoptar medidas de seguridad que redundarán en beneficios para todos."

Así mismo el protocolo IPv6 debido a su gran cantidad de direcciones disponibles no tiene como política manejar direcciones IP públicas o privadas, por lo que elimina toda clase de elementos que permite "esconder" direcciones IP públicas en la comunicación (como uso de NATs – Traducciones de red)), lo cual minimiza los riesgos de intrusión en la red; sin embargo lo anterior no quiere decir que el protocolo IPv6 sea más seguro que IPv4, pero el IPv6 si obliga a incorporar dentro del paquete IP al protocolo IPsec (eliminando la variedad de protocolos de seguridad existentes en IPv4), y al no requerir NATs, se puede utilizar IPsec, extremo-a-extremo, incrementando los niveles de seguridad en la red."

Direccionamiento IP

✓ Para el comportamiento del tráfico de IPv6, se requiere tener en cuenta el uso de las directivas de seguridad del protocolo IPsec, para ambientes que requieren atender solicitudes de servicios HTTP entre nodos IPv6.

✓ Considerar la revisión de los segmentos de bloque de direcciones en IPv6 y si estos se ha realizado por zonas lógicas de seguridad (Zonas Desmilitarizadas – DMZ) con base en las necesidades de operación de cada organización y estableciendo los criterios de seguridad correspondientes.

✓ La utilización de los bloques de direccionamiento en IPv6, deben acoger las políticas de seguridad y privacidad de la información permitiendo que el funcionamiento de las mismas sea transparente para los usuarios finales de la Entidad.

✓ Los planes de direccionamiento en IPv6 se deben realizar con base en los criterios de confidencialidad, integridad y disponibilidad de los sistemas de información y comunicaciones.

✓ La utilización del direccionamiento IPv6 debe utilizarse en forma espaciada y no consecutiva como recomendación general a fin de evitar ataques de direccionamiento IP tanto del interior como del exterior en modalidad de "fuerza bruta".

Se recomienda crear VLANs (Redes de Área Local Virtuales) por separado dentro de las redes locales de las organizaciones para propósitos de pruebas de direccionamiento, tráfico, monitoreo y seguridad cuando se comience la fase de implementación del nuevo protocolo.

✓ En redes IPv6 los paquetes pasan por distintas etapas de enrutamientos, con el fin de mitigar el espacio de búsqueda de posibles atacantes de escaneo sobre las redes IPv6, por lo tanto se recomienda que los administradores de las redes utilicen herramientas de software de monitoreo para controlar posibles patrones de comportamiento de direccionamiento IP aún si el tráfico generado es dirigido (multicast) y se utiliza descubrimiento de vecinos (Neighbor discovery)4.

✓ Los paquetes IPv6, deben seguir las recomendaciones de seguridad de los paquetes IPv6, consistente en que estos contienen cabeceras de autenticación (AH, Authentication Headers) y encabezados de extensión de carga de seguridad encapsulada (ESP, Encapsulating Security Payload), en la cual el protocolo IPsec permite para cualquier nodo de IP el establecimiento de sesiones de seguridad de extremo a extremo.

En el momento el Instituto se encuentra estudiando la implementación del IPV6.

22. LINEAMIENTOS: TERMINALES DE ÁREAS FINANCIERAS ENTIDADES PÚBLICAS

- ✓ **Lineamientos**

A continuación se presentan los requerimientos mínimos en seguridad de la información e informática que deben cumplir las entidades públicas de orden nacional y orden territorial en cuanto a los equipos o terminales móviles utilizados para la realización de transacciones financieras con recursos públicos, a través de los portales de internet que las entidades bancarias disponen para tal fin.

- ✓ **Lineamientos de Seguridad Lógica**

La entidad deberá asegurarse de lo siguiente:

a) Requerir credenciales de autenticación para el ingreso y/o uso, las cuales deberán estar obligadas a cambiarse periódicamente y tener especificaciones mayores de seguridad (longitud mínima de ocho caracteres alfanúmeros y caracteres especiales) de conformidad con la tecnología y mecanismos técnicos que dispongan las instituciones financieras para este fin.

b) Controlar el tiempo de inactividad del usuario a través de bloqueo automático del equipo o terminal móvil (se sugiere máximo cinco minutos).

c) Limitar los privilegios de la(s) cuenta(s) de usuario(s) utilizada(s) para realizar transacciones financieras en los equipos y/o terminales para este fin, a efecto de reducir el riesgo de que con la misma sea posible la instalación de software malintencionado o controladores de dispositivos no autorizados.

d) Restringir en lo posible la ejecución de archivos como (.exe, .vbs, .com .scr, etc.) que no hagan parte de los sistemas necesarios para la elaboración de las actividades propias del cargo y que hayan sido descargados de sitios web o recibidos vía correo por parte del usuario del equipo por medio del cual se realizan las transacciones financieras.

e) Establecer procedimientos automatizados o por medio del soporte técnico que disponga la entidad, para efectuar el borrado regular de: archivos temporales del sistema operativo, archivos temporales de Internet, cookies, historial de navegación y descargas (se sugiere mínimo una vez a la semana).

f) Establecer los mecanismos necesarios para que la instalación, actualización o desinstalación de programas o dispositivos en el equipo o terminal móvil, sea realizada únicamente por los funcionarios del área de sistemas o tecnología, o el personal designado por la Entidad para este tipo de requerimientos.

adicionalmente, estas actividades deben ser revisadas y aprobadas por el funcionario que desempeñe el rol de oficial de seguridad de la información, y/o las áreas responsables de la seguridad de la información y/o los designados por la entidad para efectuar este tipo de aprobaciones.

g) Restringir la instalación de software que permita conexión remota (TeamViewer, LogMeIn, Hamachi, VCN, entre otros) evitando con esto que personas externas se puedan conectar fácilmente al equipo o terminal desde el cual se realizan las transacciones.

h) Asegurar que el equipo y/o terminal móvil cuente mínimo con: antivirus (con módulos de anti - keylogger, firewall personal, antispyware), software licenciado y actualizado de forma automática o supervisada.

i) Restringir los puertos que permitan la conexión y/o acceso a dispositivos de almacenamiento extraíbles (CD, USB, SD Card, etc.).

j) Restringir el software de acceso remoto al equipo que pueda ofrecer o tener preinstalado el Sistema Operativo del respectivo equipo o terminal.

k) Procurar tener instalado un solo navegador, en el que esté comprobada la adecuada compatibilidad y operación de servicios en línea de las instituciones financieras con las que tenga relación, con mejores mecanismos de seguridad posibles debidamente configurados y el cual deberá estar permanentemente actualizado a efecto de garantizar la disposición de mejoras o correcciones a su funcionamiento.

l) Activar mecanismos para que el equipo o terminal pueda recibir las actualizaciones de seguridad de forma automática, cada vez que sean emitidas por el fabricante para el sistema operativo respectivo y aplicaciones.

m) Mantener activos y en operación sólo los protocolos, servicios, aplicaciones, usuarios, entre otros, necesarios para el desarrollo de las actividades, en el equipo o terminal.

n) En lo posible, el equipo o terminal deberá ser destinado de manera exclusiva para la realización de las transacciones financieras.

o) En lo posible, apagar el equipo o terminal cuando no se esté utilizando, sobre todo si dispone de una conexión permanente a Internet.

- ✓ **Lineamientos de Seguridad Física**

Las entidades deben asegurar que el acceso físico a las áreas donde estén los equipos o terminales móviles, sea lo más restringido posible y de manera exclusiva al responsable directo de la realización de las transacciones.

A continuación se listan los controles a ser implementados:

a) Restringir el acceso al área física desde donde se realizan transacciones financieras sólo para personal autorizado.

b) Limitar el uso de las terminales móviles corporativas al interior de la entidad, si excepcionalmente la terminal móvil debe llevarse fuera de la entidad, deberán tomarse las precauciones necesarias para evitar el acceso al mismo por parte de personas no autorizadas, o en caso de pérdida o hurto y deberán mantenerse separados de mecanismos de seguridad que habiliten la ejecución de las transacciones.

c) En lo posible, contar con cámaras de video, las cuales deben cubrir al menos el acceso principal al área y el funcionario que utilice el equipo o terminal móvil. Las imágenes deberán ser conservadas por lo menos seis (6) meses o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación,

queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

- ✓ **Lineamientos de Seguridad de la Red**

a) Restringir el acceso a correos personales, redes sociales, y en general a otros sitios no asociados con las funciones del operador, desde el equipo y/o terminal. Esto con el objeto de evitar que de forma intencional o accidental, se descargue, instale o ejecute software malintencionado.

b) Implementar mecanismos de autenticación que permitan confirmar que el equipo o terminal móvil es un dispositivo autorizado dentro de la red de la entidad.

c) Deberá evitarse realizar transacciones financieras desde dispositivos móviles o conexiones a redes inalámbricas de terceros no confiables.

d) Asegurar las redes inalámbricas (WIFI) desde las cuales se realicen transacciones financieras, cuenten con las mejores condiciones y estándares técnicos disponibles. Definir un usuario con contraseña robusta y cambiarla periódicamente.

e) Si la entidad cuenta con una red inalámbrica (WIFI) para invitados, esta deberá estar totalmente aislada y segmentada de las redes LAN de la entidad.

- ✓ **Lineamientos de Seguridad frente a la Entidad Financiera**

a) Asignar una dirección IP fija pública al equipo o terminal móvil, la cual debe ser informada a la(s) entidad(es) financiera(s), de forma que solo esta dirección IP fija sea la utilizada para realizar transacciones en los portales empresariales.

b) Garantizar la protección de las claves y dispositivos de acceso al equipo o terminal móvil y al portal empresarial de la entidad financiera. En desarrollo de

esta obligación, las entidades deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en el equipo y/o terminal móvil de la entidad deberá ser única y personalizada.

c) Utilizar las medidas de autenticación y control que le ofrecen la(s) entidad(es) financieras a través de la(s) cuales realizan transacciones. Particularmente, definir perfiles de autorización de transacciones, utilizar la preinscripción de beneficiarios, parametrizar montos y horarios para la realización de operaciones y realizar la inscripción para recibir notificaciones en línea.

- ✓ **Lineamientos de Seguimiento y Monitoreo de Controles**

a) El máximo responsable del área financiera de la Entidad, deberá coordinar con las áreas de TI y/o de seguridad de la información y/o las Oficinas de Control Interno, el responsable de verificar el cumplimiento de las condiciones de seguridad del equipo y en general, las consagradas en este instructivo, al menos cada tres (3) meses.

b) Para la verificación del cumplimiento de las condiciones de seguridad y los lineamientos aquí establecidos, se deberá diligenciar el anexo adjunto a este documento, el cual deberá ser suscrito tanto por el responsable del área financiera, como por el designado para la respectiva verificación.

- ✓ **Recomendaciones de Seguridad en la Realización de las Transacciones**

a) Acceder a la página de la entidad financiera o a través de la cual va a realizar la transacción únicamente digitando la dirección en el navegador. Nunca realice esto a través de links, motores de búsqueda o de los favoritos o marcadores del navegador.

b) Siempre cerrar la sesión del portal transaccional al terminar las transacciones.

c) En lo posible y teniendo en cuenta la afectación de algún servicio, parametrizar ante su banco de tal manera que ninguna transacción financiera pueda realizarse antes de las 6:00 a.m. y después de las 8:00 p.m., ni durante los fines de semana y/o días festivos.

d) Asegurar la restricción en el acceso a los portales transaccionales de los usuarios durante sus períodos de vacaciones o licencias y darlos de baja en casos de traslado o retiros.

e) Llevar un adecuado control de los usuarios y perfiles del equipo. Estos deben ser personalizados y de uso restringido al funcionario asignado (debe prohibirse el uso de usuarios y claves por parte de personas diferentes a la que asignaron).

f) Mantener los mecanismos de comunicación con la(s) entidad(es) financiera(s) actualizados, con el fin de informar inmediatamente en caso de identificar algún evento de riesgo que tenga relación las transacciones financieras (ej. pérdida de token, vulneración de clave, solicitud reiterada de credenciales, demoras y retardo en respuestas del Portal, mensajes de mantenimiento, notificaciones de ingresos y transacciones no reconocidas, etc.).

g) Asegurar que las personas que realizan transacciones financieras con los recursos de la entidad cuentan con capacitación en relación con la seguridad de la información y de las medidas que debe adoptar para mitigar los riesgos de fraude financiero.

INFITULUA EICE, está en proceso de implementar la lista de chequeo.

d. Mejora Continua

Una vez realizado el seguimiento, evaluación, análisis y monitoreo de los indicadores de Seguridad de la información, es necesario, continuar con la Fase Mejora. La aplicación de esta fase, le permitirá a la Entidad a partir de los resultados de la Fase de Gestión, corregir de ser necesario, los errores cometidos, así como mejorar las acciones llevadas a cabo en las fases anteriores, llevando a cabo el plan de mejoramiento continuo de seguridad y privacidad de la información. Para la definición el plan de mejora continua, se debe tener en cuenta:

- ✓ **No Conformidades y Acciones Correctivas**

- ✦ En caso de presentarse no conformidades en las auditorías realizadas, la Entidad deberá llevar a cabo las acciones necesarias para controlarlas y corregirlas.

- ✦ Evaluar y revisar la raíz de la no conformidad con el fin de eliminar las causas de la misma y evitar que vuelva a presentar. Es importante, que se verifique si existen no conformidades similares en auditorías previas.

- ✦ Comparar las no conformidades presentadas con las acciones correctivas tomadas; esto, con el fin de asegurar que no se vuelvan a presentar y evaluar la efectividad de las acciones correctivas aplicadas.

- ✦ Implementar las acciones que sean necesarias.

- ✦ Evaluar la efectividad de las acciones correctivas tomadas. - Realizar los cambios en el sistema que sean necesarios.

Así las cosas, la Entidad procederá a documentar lo sucedido de la siguiente manera:

- Evidencia de las no conformidades y acciones correctivas llevadas a cabo.
- Resultados de las acciones correctivas ejecutadas.
- Ajustar los entregables que sean objeto de modificación en el modelo de Seguridad y Privacidad de la Información.

✓ **Mejora Continua**

Es claro que el Sistema de gestión es cíclico y deberá estar en continua revisión por parte de la Entidad. La Entidad deberá mejorar continuamente la gestión del sistema a fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información.

Una vez sean mejoradas las actividades que correspondan, éstas serán incluidas en el plan de comunicaciones de la entidad a fin de que sea conocida por todos los grupos de interés.

La entidad identificará las oportunidades de mejora, conforme a los criterios de calidad establecidos en su Modelo de Gestión, a fin de enfocar sus esfuerzos en la mejora de los procesos de la misma.

23. EVALUACIÓN DESEMPEÑO

la fase de Evaluación de Desempeño es la fase donde se establecen los aspectos a ser desarrollados por los responsables de la gestión de seguridad de la información en todos los niveles de la entidad, para así, evaluar y en donde sea aplicable, medir el desempeño del sistema contra la política, los objetivos y la experiencia práctica de la gestión de seguridad de la información, a la vez que se reportan los resultados a la dirección para su revisión y toma de decisiones.

REVISION Y SEGUIMIENTO DEL MSPI

En la definición del Modelo de Seguridad y Privacidad de la Información, la fase de evaluación del desempeño hace parte de la etapa de Verificar, donde se establecen los aspectos a ser desarrollados por los responsables de la gestión de seguridad y privacidad de la información en todos los niveles, para así, evaluar y en donde sea aplicable, medir el desempeño del sistema contra la política, los objetivos y la experiencia práctica de la gestión de seguridad de la información, a la vez que se reportan los resultados a la dirección para su revisión y toma de decisiones.

Para el cumplimiento de esta fase, la organización deberá desarrollar un conjunto de actividades de seguimiento donde se mantenga de manera continua la medición y verificación del cumplimiento de los aspectos planteados en la fase de Planificación del modelo y la forma como estas actividades se han ido desarrollando o ejecutando.

Cabe notar, que estos aspectos de seguimiento y revisión deberán ser desarrollados con base en los resultados obtenidos; y se deberán ajustar los aspectos necesarios para que la seguridad y privacidad de la información sea eficiente y eficaz en el cumplimiento de los objetivos y metas trazados en la fase de planificación. Para la fase de seguimiento y revisión las actividades detalladas a continuación, tendientes a la definición de procedimientos operacionales documentados.

REVISIÓN

Se deben llevar a cabo las siguientes actividades de revisión:

- ✓ De la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.

- ✓ De la evaluación de los riesgos desarrollada en la entidad, donde a su vez se validen los niveles aceptables de riesgo y el riesgo residual después de la aplicación de controles y medidas administrativas.

SEGUIMIENTO Se deben llevar a cabo actividades para realizar seguimiento a:

- ✓ La programación y ejecución de las actividades de auditoria interna del MSPI
- ✓ La programación y ejecución de las revisiones por parte del encargado de seguridad y privacidad de la información.
- ✓ El alcance del MSPI y las mejoras del mismo.
- ✓ Los planes de seguridad tanto para el establecimiento como la ejecución y actualización de los mismos, como respuesta a los aspectos identificados a nivel de las revisiones y seguimientos realizados en esta fase de implementación.
- ✓ A los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o el desempeño de la seguridad y privacidad de la información.

ACTIVIDADES GENERALES DE SEGUIMIENTO Y REVISIÓN Las siguientes son las actividades generales que soportan la etapa de Evaluación del Desempeño del MSPI:

- Revisión de la eficacia del MSPI.
- Medición de la efectividad de Controles.
- Revisión de las valoraciones de los riesgos.
- Medición de los indicadores de gestión del MSPI.

• Realización de auditorías.

• Revisiones del MSPI por parte de la dirección.

• Actualizar los planes de seguridad.

• Registro de las actividades del MSPI.

• Revisiones de Acciones o Planes de Mejora (Respuesta a no conformidades).

Desde el punto de vista del desarrollo de estas actividades, su cumplimiento deberá estar enmarcado en el modelo PHVA al interior de los procesos, donde se integran los aspectos de la gestión de la organización que establece para las etapas de verificación las siguientes tareas:

• Consolidar indicadores periódicamente.

• Evaluar indicadores frente a las metas.

• Graficar los Indicadores.

• Analizar causas de las desviaciones.

• Evaluar las No Conformidades ocurridas y su impacto en el cumplimiento de las metas y objetivos del MSPI.

24. DOCUMENTACIÓN DE LA ETAPA DE EVALUACIÓN DEL DESEMPEÑO

En esta etapa se definen las actividades que permiten medir el avance de los elementos definidos en la etapa anterior, se deben generar o actualizar los siguientes documentos necesarios para el MSPI:

• Revisión de la eficiencia del MSPI

- Medición de efectividad de controles
- Revisión de valoraciones de riesgos
- Realización de auditorías internas
- Revisiones del MSPI por la dirección
- Actualización de los planes de seguridad
- Registro de actividades del MSPI
- Revisiones de acciones o planes de incidentes

25. GESTIÓN DE INCIDENTES

Este anexo entrega los lineamientos básicos para poner en marcha un Sistema de Gestión de Incidentes de Seguridad de la información, a través de un modelo propuesto, el cual está concebido para que se puedan integrar los incidentes de seguridad sobre los activos de información, independiente del medio en el que se encuentren.

✓ **Objetivo**

El objetivo principal del Modelo de Gestión de Incidentes de seguridad de la información es tener un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información.

Los objetivos del modelo son garantizar que:

✓ Definir roles y responsabilidades dentro de la Organización como eje puntual para evaluar los riesgos y permita mantener la operación, la continuidad y la disponibilidad del servicio.

- ✓ Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- ✓ Permitir identificar los incidentes de seguridad de la información para ser evaluados y dar respuesta de la manera más eficiente y adecuada.
- ✓ Minimizar los impactos adversos de los incidentes en la organización y sus operaciones de negocios mediante las salvaguardas adecuadas como parte de la respuesta a tal incidente.
- ✓ Consolidar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para aprender rápidamente. Esto tiene como objeto incrementar las oportunidades de prevenir la ocurrencia de futuros incidentes, mejorar la implementación y el uso de las salvaguardas y mejorar el esquema global de la gestión de incidentes de seguridad de la información.
- ✓ Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y registro de incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.
- ✓ Definir los procedimientos formales de reporte y escalada de los incidentes de seguridad.
- ✓ Establecer variables de posible riesgo, en efecto, es la posible valoración de aspectos sensibles en los sistemas de información.

Para lograr estos objetivos, la gestión de incidentes de seguridad de la información involucra los siguientes procesos de manera cíclica como lo muestra la imagen:

- ✓ Planificación y preparación para la gestión del Incidente
- ✓ Detección y análisis.
- ✓ Contención, erradicación y recuperación.
- ✓ Actividades Post-Incidente.

Esta guía le permitirá a las entidades estar preparadas para afrontar cada una de las etapas anteriores, y adicionalmente definiendo responsabilidades y procedimientos para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

- ✓ **Características de un Modelo de Gestión de Incidentes**

Esta guía de gestión de incidentes de seguridad de la información plantea una serie de actividades para dar cumplimiento con el ciclo de vida de la gestión y respuesta a un incidente de seguridad.

Para definir las actividades de esta guía se incorporaron componentes definidos por el NIST alineados con los requerimientos normativos de la NTC–ISO–IEC 27035-2013 para la estrategia de Gobierno en Línea.

Es recomendable que las entidades creen un equipo de atención de incidentes de seguridad en cómputo CSIRT o un grupo que haga sus veces, quienes se encargaran de definir los procedimientos a la atención de incidentes, realizar la atención, manejar las relaciones con entes internos y externos, definir la clasificación de incidentes, y además de esto se encargaran de:

- Detección de Incidentes de Seguridad: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
- Atención de Incidentes de Seguridad: Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
- Recolección y Análisis de Evidencia Digital: Toma, preservación, documentación y análisis de evidencia cuando sea requerida.
- Anuncios de Seguridad: Deben mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación (Web, Intranet, Correo).
- Auditoria y trazabilidad de Seguridad Informática: El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.
- Certificación de productos: El equipo verifica la implementación de las nuevas aplicaciones en producción para que se ajusten a los requerimientos de seguridad informática definidos por el equipo.

- Configuración y Administración de Dispositivos de Seguridad Informática: Se encargaran de la administración adecuada de los elementos de seguridad informática.
- Clasificación y priorización de servicios expuestos: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
- Investigación y Desarrollo: Deben realizar la búsqueda constante de nuevos productos en el mercado o desarrollo de nuevas herramientas de protección para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad de la información.

Este grupo está enfocado principalmente en atender los incidentes de seguridad de la información que se presentan sobre los activos soportados por la plataforma tecnológica de la entidad.

En este momento en INFITULUA EICE existe un formato para Gestión de Incidentes, pero no un procedimiento como tal, es importante adoptar las medidas comprendidas en este punto del manual.

26. GLOSARIO

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante.

o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000)

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información: SGSI Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.