PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia | Nit: 892400461-5 | Teléfonos: (57. 8) 5121350 - 51266 07 | Fax: 512 57 70 | Email: info@infotepsai.edu.co | www.infotepsai.edu.co |
Vigilada MinEducación

Contenido

1. INTRODUCCION 3
2. OBEJTIVO 3
3. ALCANCE 4
4. DEFINICIONES: 4
5. REFERENCIAS NORMATIVAS 6
6. ADMINISTRACIÓN DEL RIESGO 7
7. POLITICA DE ADMINISTRACION DEL RIESGO 8
8. GESTION DEL RIESGO 8
9. CONTEXTO ESTRATEGICO 11
10. ANALISIS DE RIESGOS 11
11. IDENTIFICACIÓN DEL RIESGO 11

11.2 IDENTIFICACION DE LOS ACTIVOS 12

11.3 IDENTIFICACION DE LAS AMENAZAS 12

12. Actividades: ..... **¡Error! Marcador no definido.**

1. INTRODUCCION

Instituto de Nacional de Formación Técnica Profesional INFOTEP. Es una Institución de Educación Superior, que ofrece formación técnica profesional, programas académicos en extensión orientados bajo los principios y valores institucionales, hacia la formación integral para toda la población del departamento insular y el caribe, buscando el desarrollo social, económico, científico, cultural, tecnológico y ambiental a través de la investigación; generando proyectos en alianza con el estado, sector productivo, los gremios, y otras instituciones, con talento humano idóneo, dando como resultado profesionales integrales, pensantes, emprendedores y formadores de una mejor calidad de vida con el trilingüismo como identidad cultural y proyección social para el Archipiélago.

Los cambios generados por la evolución continua de las tecnologías de la información y las comunicaciones, y en general de las redes informáticas, han inclinado a algunas entidades y ciudadanos a utilizarlas como medios para incrementar su productividad, para ser más competitivos en los negocios, para satisfacer necesidades propias y para generar valor. Por otra parte, en otros escenarios se ha incrementado el uso de la tecnología con fines delictivos o para generar amenazas informáticas; este propósito busca afectar otras infraestructuras tecnológicas, sistemas de información financieros, personas e, incluso, llegar a impactar la economía de toda una nación. Es por esta razón, que los estados han incrementado su preocupación por los riesgos a los que puedan estar expuestas las instituciones (entidades, organizaciones, empresas y la misma ciudadanía) y han decidido incluir en sus planes estratégicos, modelos de seguridad de la información y políticas de seguridad digital encaminados básicamente a fortalecer la seguridad y por ende, de todos los que la componen.

Por tal motivo INFOTEP Archipiélago se alinea con el Marco Normativo vigente para el diseño e implementación del plan de tratamiento de riesgos con el fin de identificar y evaluar los riesgos inherentes a la seguridad de la información con base en el Modelo de Seguridad y Privacidad del estado colombiano, decretos, políticas, conpes que alinean a las entidades hacia una adecuada gestión del tratamiento de los riesgos en entidades publicas

2. OBEJTIVO

Establecer los criterios institucionales que orienten al INFOTEP en la correcta identificación, análisis, valoración y administración de los riesgos relacionados con la seguridad de la información que pueden afectar los objetivos institucionales.

3. ALCANCE

Los lineamientos de este documento deben ser aplicados en todos los procesos de la institución. Esta guía, proporciona la metodología establecida por el INFOTEP para la administración y gestión de los riesgos a nivel de procesos.

4. DEFINICIONES:

- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información*; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información.*
- **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación
- **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.

- **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.

- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

- **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.

- **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

- **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.

- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

- **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos

- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

- **Mapa de riesgos:** documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

- **Materialización del riesgo:** ocurrencia del riesgo identificado

- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).

- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio

- **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

- **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.

- **Proceso:** conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

- **Riesgo de corrupción:** posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

5. REFERENCIAS NORMATIVAS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

- Decreto 2573 de 2014. Gobierno en Línea
- Decreto 1008 de 2018. Política de Gobierno Digital
- CONPES 3854 de 2016. Política nacional de Seguridad Digital

6. INTERACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CON EL MODELO DE GESTION DE RIESGOS DE SEGURIDAD DIGITAL.

El MSPI integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad digital, ya que esta práctica constituye su base fundamental. La guía para la gestión del riesgo, llevarán a cumplir dichas tareas de gestión de riesgo de seguridad digital requeridas en el MSPI.
En esencia, la interacción entre ambos modelos puede resumirse de la siguiente manera:

1. Las actividades de identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos se alinean con la fase de PLANIFICACIÓN del MSPI.
2. Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de IMPLEMENTACIÓN del MSPI.
3. Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la fase de MEDICIÓN DEL DESEMPEÑO del MSPI.
4. Las actividades de MEJORAMIENTO CONTINUO en ambos modelos son similares y trabajan simultáneamente, ya que dependerán de las fases de Medición del Desempeño para identificar aspectos a mejorar en la aplicación de ambos Modelos.

7. ADMINISTRACIÓN DEL RIESGO

La **Administración de riesgos** es un término aplicado a un método lógico y sistemático de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los **riesgos** asociados con una actividad. Este concepto debe ser tenido y ser aplicado en el INFOTEP dado que este se encuentra expuesta a diferentes riesgos o eventos que pueden poner en peligro su existencia.

Los sistemas de gestión basados en riesgos funcionan como una herramienta preventiva, cuando se administran los riesgos de una manera adecuado se logra una mejor planificación lo cual conlleva lograr los objetivos de la institución. Los Jefes de la institución son las personas encargadas de liderar la administración del riesgo.

8. POLITICA DE ADMINISTRACION DEL RIESGO

El INFOTEP se compromete a controlar los riesgos que puedan impedir el cumplimiento de los objetivos institucionales para ello realiza una adecuada administración de los mismos por medio de cada uno de sus funcionarios los cuales dentro de cada proceso deben identificarlos y evitar su materialización.

Se deberían identificar los riesgos que puedan generar mayor impacto en el INFOTEP y que afecten los servicios para el cumplimiento de la misión y objetivos del INFOTEP.

Dentro de la política las opciones de tratamiento del riesgo según la norma ISO 31000

- Aceptación del riesgo.
- Rechazo del riesgo.
- Transferencia del riesgo.
- Mitigación del riesgo.

9. GESTION DEL RIESGO

Son actividades coordinadas para identificar, analizar, valorar, dar tratamiento y monitorear los riesgos que pueden afectar los objetivos de la institución.

Proceso para la administración del riesgo:

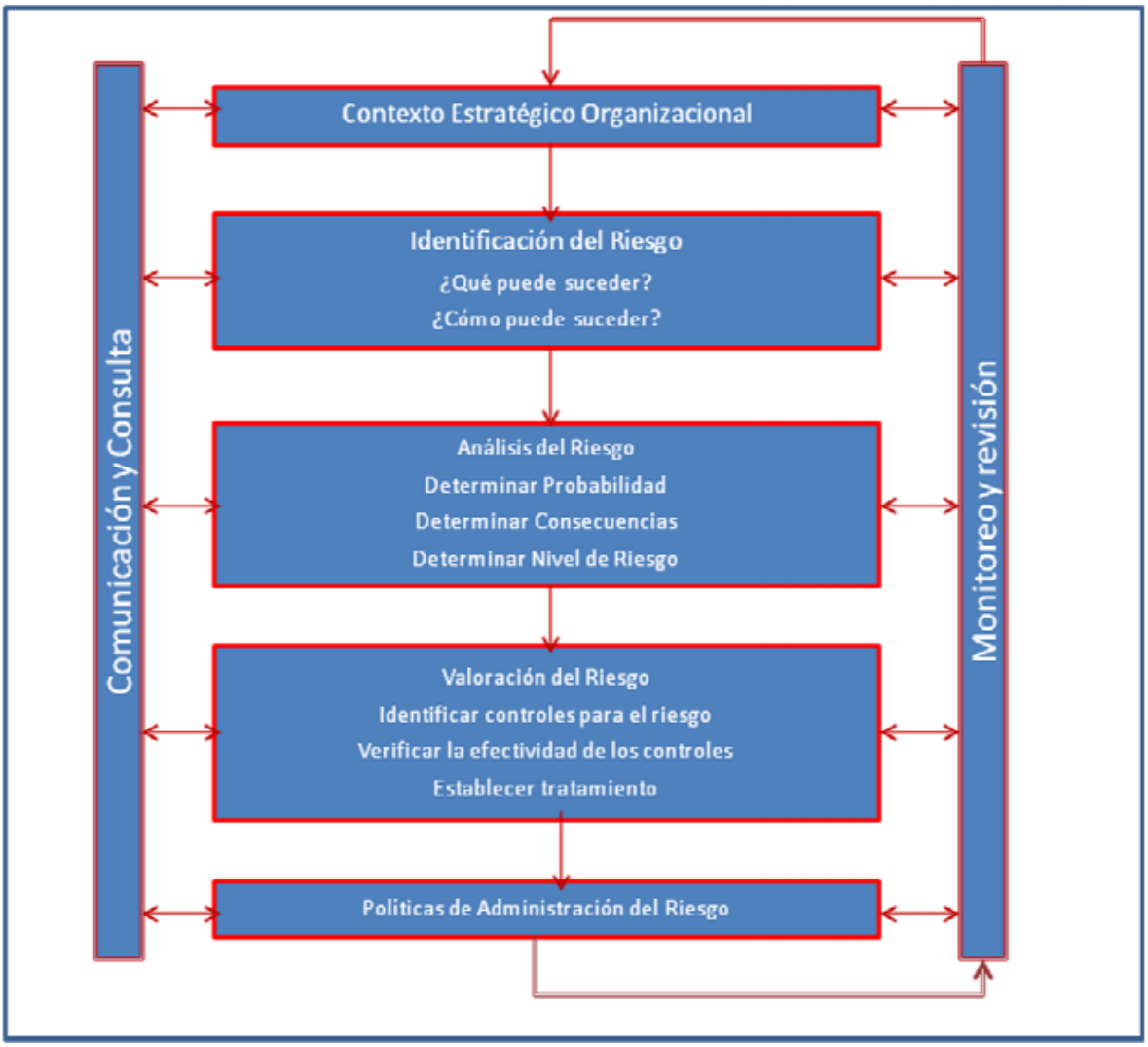

Imagen 1. Tomado de la Cartilla de Administración de Riesgos del D

- Proceso para la administración del riesgo en seguridad de la información

  A continuación se muestra el diagrama de flujo correspondiente al ciclo de vida durante la administración de los riesgos de seguridad de la información

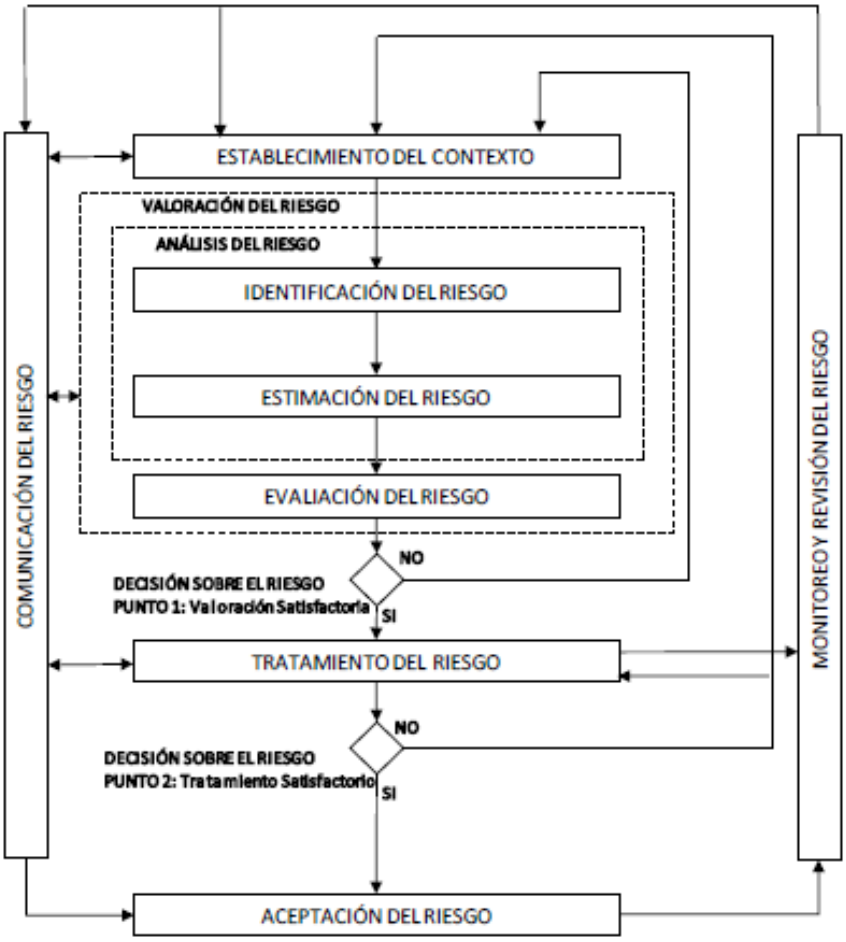

Imagen 2. Tomado de la NTC-ISO/IEC 27005

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI.

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Tabla 3. Etapas de la Gestión del Riesgo a lo Largo del MSPI

10. CONTEXTO ESTRATEGICO

El Instituto Nacional de Formación Técnica Profesional busca Desarrollar una cultura investigativa en la comunidad educativa del Departamento que facilite el acceso al conocimiento científico, tecnológico y técnico, para dar respuestas adecuadas y pertinentes a las problemáticas de su entorno que sean afines a los campos disciplinares. Para cumplir tales objetivos la institución debe tener una adecuada administración de los riesgos institucionales y los de corrupción.

La administración adecuando de los riesgos de la seguridad de la información en la institución tiene como propósito dar soporte al modelo de seguridad de la información al interior del INFOTEP, conformidad legal y evidencia de la debida diligencia.

11. ANALISIS DE RIESGOS

Para el INFOTEP es muy importante documentar y especificar cada una de las etapas surtidas para el proceso de Gestión de Riesgos, de allí el INFOTEP tendrá su propia guía para poder replicar este mismo procedimiento para cualquier etapa que sea necesaria, ya sea para el momento en el que el INFOTEP decida extender el alcance de la aplicación del MSPI, o para la etapa de revisión de los controles, en la cual el INFOTEP sólo debería poder aplicar la misma metodología simplemente teniendo como base el trabajo ya adelantado en las primeras etapas del MSPI.

12. IDENTIFICACIÓN DEL RIESGO

Permite identificar los riesgos que pueden afectar el cumplimiento de la misión de la institución dado que en el momento en que se materialice uno de ellos afectarían la confidencialidad, la integridad o la disponibilidad de los activos de información de la institución.

Clasificación de los riesgos

1. Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

2. Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

3. Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

4. Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

5. Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

6. Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

12.2 IDENTIFICACION DE LOS ACTIVOS

Se identificaron varios grupos de activos de información tales como:

CENTRO DE DATOS
Bases de datos
Servidores
Almacenamiento
Red de datos
Pcs

12.3 IDENTIFICACION DE LAS AMENAZAS

Las amenazas son todas aquellas cosas que tienen el potencial de causar daños a los activos como información, procesos y sistemas. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas.

A continuación se describen una serie de amenazas comunes.

D= Deliberadas, A= Accidentales, E= Ambientales

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológico	E
	Inundación	E
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	E
	Perdida de suministro de energía	E
	Falla en equipo de telecomunicaciones	
Perturbación debida a la radiación	Radiación electromagnética	
	Radiación térmica	
	Impulsos electromagnéticos	
Compromiso de la información	Interceptación de señales de interferencia comprometida	
	Espionaje remoto	
	Escucha encubierta	
	Hurto de medios o documentos	
	Hurto de equipo	
	Recuperación de medios reciclados o desechados	
	Divulgación	
	Datos provenientes de fuentes no confiables	
	Manipulación con hardware	
	Manipulación con software	
	Detección de la posición	
Fallas técnicas	Fallas del equipo	
	Mal funcionamiento del equipo	
	Saturación del sistema de información	
	Mal funcionamiento del software	
	Incumplimiento en el mantenimiento del sistema de información.	

Acciones no autorizadas	Uso no autorizado del equipo	
	Copia fraudulenta del software	
	Uso de software falso o copiado	
	Corrupción de los datos	
	Procesamiento ilegal de datos	
Compromiso de las funciones	Error en el uso	
	Abuso de derechos	
	Falsificación de derechos	
	Negación de acciones	
	Incumplimiento en la disponibilidad del personal	

Tabla 2: Amenazas Comunes

Es recomendable tener particular atención a las fuentes de amenazas humanas. Estas se desglosan específicamente en la siguiente tabla:

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Guerra de la información • Ataques contra el sistema DDoS • Penetración en el sistema • Manipulación en el sistema
Espionaje industrial(inteligencia, empresas, gobiernos	Ventaja competitiva Espionaje económico	• Ventaja de defensa • Ventaja política • Explotación económica

extranjeros, otros intereses)		• Hurto de información • Intrusión en privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	Asalto a un empleado Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto Soborno de información Ingreso de datos falsos o corruptos Interceptación Código malicioso Venta de información personal Errores en el sistema Intrusión al sistema Sabotaje del sistema Acceso no autorizado al sistema.

13. PLAN DE COMUNICACIONES

El plan de comunicación o capacitación debe ser un medio para la mejora en las diferentes áreas funcionales que componen la Institución. Bajo esta premisa a continuación se especifican los objetivos del Plan, en función de lo que se pretende implementar en el Modelo de Seguridad y Privacidad de la Información.

De manera concreta los objetivos definidos para este plan de son:

Integración del Departamento. Apoyar por medio de capacitación continua, la integración efectiva de las diferentes áreas funcionales que componen la integración del área de las Tecnologías de Información con el Modelo de Seguridad de la Información. Este proceso de capacitación debe permitirles a los funcionarios respectivos un claro entendimiento de las funciones y responsabilidades de cada participante bajo el Modelo de Seguridad de la Información para mejor prestación de servicios, así como el dominio de los mecanismos de retroalimentación respectivos.

Utilización eficiente de métodos y herramientas. Este proceso de capacitación debe apoyar el uso eficiente de los diferentes métodos y herramientas que se requieren aplicar en la prestación de servicios de la Institución. Esta capacitación no solo

comprende las áreas técnicas del servicio, sino también los componentes administrativos y del negocio que se consideran necesarios para lograr un mejoramiento continuo.

Aprovechamiento de los servicios tecnológicos. El proceso de capacitación debe apoyar el uso eficiente e integral de los servicios tecnológicos para las diferentes áreas con el fin de que cada funcionario no sea un eslabón que genere debilidades en el Modelo de Seguridad que se pretende implementar.

Evolución del servicio brindado. El proceso de capacitación debe apoyar la creación y mantenimiento de canales de comunicación enfocados al mejoramiento y actualización continua de las técnicas y herramientas utilizadas para proteger la información.

Retención y atracción de personal. El proceso de capacitación debe propiciar la profesionalización de los recursos del proceso, así como un ambiente tecnológicamente seguro para los usuarios internos y externos. Esta característica permitirá controlar de manera más efectiva la eventual rotación de personal, la búsqueda y consolidación del personal contratado.

Redes Sociales. Mejoraramiento de los niveles de seguridad que gestiona cada usuario interno y externo de la institución en Facebook y generar nuevos canales de comunicación (Twitter, Instagram) reutilización del canal de youtube como metodología para apropiar y acercar a los usuarios a interactuar en un ambiente seguro.

14. SEGUIMIENTO DE RIESGOS Y REVISIÓN

El INFOTEP gestionara la matriz de seguimiento a los riesgos y revisiones que se adelantaran con base en las referencias normativas en el desarrollo de este proceso.