PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO
DIRECCIÓN TECNOLOGIA INFORMATICA

IES INFOTEP
CIENAGA, MAGDALENA
2024

www.infotephvg.edu.co
Calle 10 No. 12-22
Teléfono: (+57) 60 4240800
e-mail: ihvg@infotephvg.edu.co
quejasreclamos@infotephvg.edu.co
@infotephvg

1 OBJETIVOS

1.1 OBJETIVO GENERAL.

Establecer los lineamientos y la metodología para llevar a cabo el análisis, valoración y tratamiento de los riesgos de la seguridad de la información, el cual, debe estar alineado a la política de seguridad y privacidad de la información, así como a las definidas por la institución en el sistema integrado de gestión de la calidad con respecto a los riesgos.

1.2 OBJETIVOS ESPECÍFICOS

- Realizar una adecuada gestión de los eventos de seguridad de la información con el fin de detectar y tratar con eficiencia los incidentes que afecten la seguridad de la información de la institución.
- Establecer el alcance del plan para la gestión de los riesgos de seguridad y privacidad de la información.
- Determinar los activos de información de la IES INFOTEP, con el fin de establecer los mecanismos para su protección e identificar las principales amenazas que los afectan y de esta manera mitigar los posibles riesgos a los que están expuestos.
- Realizar la evaluación y comparación del nivel de riesgo actual con el impacto generado luego de implementar el plan de gestión de riesgos de seguridad de la información.

2 CONTEXTO

Bajo el escenario actual en el que se encuentra el mundo, principalmente el sector productivo y educativo, considerando los efectos ocasionados por la pandemia generada por el COVID-19, las tecnologías de la información y la comunicación – TIC se han convertido en elemento fundamental para garantizar la prestación de los servicios. Sin embargo, esta novedosa forma de trabajo soportada por poderosas herramientas de comunicación y de gestión, que viabilizan el desarrollo de los procedimientos y operación

de estas, además de la interacción efectiva, entre trabajadores, directivos, docentes, estudiantes y demás partes interesadas.'

En este sentido, el gobierno nacional ha establecido una serie de lineamientos para brindar a las empresas, instituciones y demás partes interesadas, estrategias para una adecuada gestión de los riesgos que atentan contra la seguridad de la información, es así, como a través de documento CONPES 3854 de 2016 estableció la política nacional de seguridad digital que busca "fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el País" 1.

Esta nueva forma de trabajo apoyada en las TIC, y soportada en la interacción a través de medios electrónicos, expone a las instituciones, organizaciones y empresas a grandes riesgos de seguridad y privacidad de la información. Por lo tanto, surge la necesidad en la IES INFOTEP de crear e implementar planes que permitan una adecuada gestión de los riesgos que atentan contra la seguridad y privacidad de la información

3 ALCANCE.

El Plan para la gestión de los riesgos de seguridad y privacidad de la información de la IES INFOTEP, aplica para todos los funcionarios, estudiantes, docentes, administrativos y contratistas de la institución. Así mismo, para la identificación, clasificación, valoración y tratamiento de los riesgos de seguridad y privacidad de la información. Este plan involucra a todos los procesos y áreas de la institución, especialmente para aquellos que impactan la consecución de los objetivos y estrategias institucionales.

4 PARAMETROS DE EJECUCIÓN

Para la ejecución del plan para la gestión de los riesgos en la seguridad y privacidad de la información, la IES INFOTEP, define los siguientes lineamientos:

- Los líderes de proceso y jefes de dependencias, junto con el director de tecnología informática de la institución son los responsables de la adecuada y oportuna aplicación de este plan.

- Para la valoración de los riesgos de seguridad de la información se debe involucrar a los líderes de proceso.

- El plan deberá estar debidamente aprobado por el ente responsable en la institución.

- Se debe ejecutar un análisis de riesgo al año, o cuando se realicen actualizaciones o cambios significativos en los procesos u operaciones institucionales. Cuya responsabilidad recae en el director de TI y la persona encargada de la oficina de planeación.

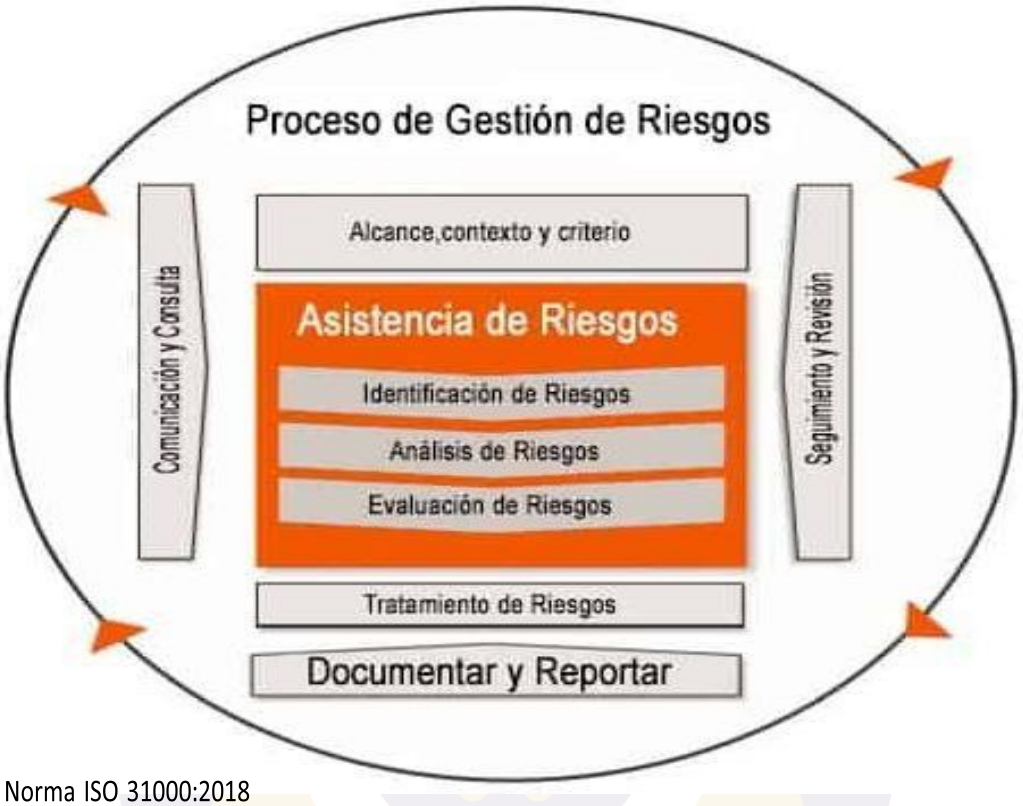
5 DOCUMENTOS RELACIONADOS.

Dentro de los documentos que se encuentran relacionados al plan para el tratamiento de los riesgos de seguridad de la información en la institución, se encuentran:

- Política de seguridad y privacidad de la información.
- Norma ISO 31000:2009
- Inventario de Activos de Información.
- Manual del Sistema Integrado para la Gestión de la Calidad.

6 METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACION.

LA IES INFOTEP, para la evaluación del riesgo de seguridad de la información toma como referente la metodología utilizada por la norma ISO 31000:2018. Por lo tanto, las actividades que hacen parte de la metodología son las siguientes:



Fuente: Norma ISO 31000:2018

En este sentido, la IES INFOTEP ha establecido que, para la gestión del riesgo de seguridad y privacidad de la información, llevará a cabo una serie de etapas que viabilizaran la identificación, evaluación, análisis, monitoreo y comunicación. Estas etapas de la metodología para la gestión del riesgo se detallan a continuación:

6.1 IDENTIFICACIÓN DE RIESGOS.

Esta etapa tiene por objetivo la identificación de los principales riesgos a la seguridad de la información a los que se encuentran expuestos los procesos de la IES INFOTEP. Esta identificación podrá realizarse de los siguientes métodos:

- Reuniones con los equipos de trabajo.
- Encuestas a las partes interesadas.

- Matrices de riesgos de ejercicios previos.

Una vez identificados los riesgos de seguridad y privacidad de la información, estos deben documentarse en una matriz de riesgos, en los que se describen y se clasifican.

6.2 VALORACIÓN DE LOS RIESGOS

En esta etapa se busca darle valor a cada uno de los riesgos identificados sobre la base de acontecimientos de seguridad de la información a los que se encuentran expuestos cada uno de los procesos de la institución y las causas que puedan comprometer la confiabilidad, integridad y disponibilidad de los activos de información. Para lo cual, es preciso que se lleven a cabo las siguientes actividades:

- Identificar los flujos de información.
- Identificar de estos flujos las vulnerabilidades existentes
- Identificar las amenazas que podrían, dadas las vulnerabilidades existentes.
- Definir las escalas a implementar.

De acuerdo con lo anterior, teniendo en cuenta los lineamientos para la gestión de riesgos digitales en entidades públicas, emitida por el DAFP, se podrán identificar los siguientes tres riesgos inherentes de seguridad digital:

- Perdida de la confidencialidad.
- Pérdida de la integridad.
- Pérdida de la Disponibilidad.

Es así, como para cada riesgo, es necesario asociar el grupo de activos específicos de cada proceso, al tiempo que se analizan las posibles amenazas y vulnerabilidades que podrían ocasionar o causar su materialización. A continuación, se presenta un listado de amenazas y vulnerabilidades que podrían materializar los tres riesgos inherentes antes mencionados:

6.2.1 Identificación de Amenazas.

Las amenazas que representan para los procesos de la IES INFOTEP situaciones o fuentes

que puedan hacer daño a los activos de información y materializar los riesgos. A continuación, se ilustran las siguientes amenazas que se pueden presentar, organizadas por tipo, amenaza y origen [deliberadas(D), fortuitas(F), Ambiental(A)]:

TIPO	AMENAZA	ORIGEN
Daño Físico	Incendios	D,F
	Inundaciones	D,F
Desastres Naturales	Fenómenos Climáticos	A
	Fenómenos Sísmicos	A
Pérdida de los servicios esenciales	Fallas en los servicios de suministro de agua	D,F
Perdida de la información	Fallas en el suministro eléctrico y de acondicionadores de aire	D,F
Perturbaciones por radiación	Radiación electromagnética	D,F
	Radiación térmica	D,F
Pérdida de la información	Interceptaciones de señales o interferencia comprometida	D
	Espionaje Interno o externo	D
Fallas Técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación de los sistemas de información	D,F
	Inconsistencia en el software por ausencia o falta de parametrización	D,F
	Incumplimiento en el Mantenimiento preventivo y correctivo a los equipos	D
Accesos no autorizados	Usos no autorizados en el equipo	D
	Uso o copia fraudulenta del software	D
Compromiso de las funciones	Usurpación de funciones	D
	Abuso de derechos	D
	Uso o copia fraudulenta del software	D
Compromiso de las funciones	Usurpación de funciones	D
	Abuso de derechos	D
	Piratería	D
	Ingeniería social	D
	Ataques por computador	D

	Fraude	D
	Ataques contra el sistema de información y la red de datos	D
	DDos	D
	Penetración en el sistema	D
	Robo de información	D
	chantaje	D

6.2.2 Identificación de Vulnerabilidades.

Para tener un referente para la definición de las vulnerabilidades, las cuales, se convierten en debilidades que pueden permitir que se materialicen los riesgos a la seguridad y privacidad de los activos de información de la institución, por lo que se presentan a continuación los siguientes tipos y su correspondiente vulnerabilidad:

TIPO	VULNERABILIDAD
Hardware	Ausencia del plan de mantenimiento preventivo y correctivo
	Ausencia del plan de renovación de equipos
	Ausencia de protocolos para la disposición final de los equipos
Software	Ausencia de Mantenimiento Preventivo y correctivo al software
	Ausencia de Licencias de Software
	Ausencia de Licencias de Antivirus
	Ausencia de Mecanismos de autenticación de usuarios
	Accesos sin Protección
Redes	Tráfico sin conexión
	Cableado y dispositivos de comunicación deficientes
	Ausencia de Mantenimiento al cableado, conectores y dispositivos de comunicación.
Humano	Falta de personal
	Falta de entrenamiento en seguridad y privacidad de la información
	Ausencia de políticas de uso de equipos
Lugar	Ausencia de protocolos para acceso a las instalaciones de la institución
	Espacios susceptibles a inundaciones, incendios
	Sistema eléctrico inestable e ineficiente y sin equipos de protección (estabilizadores de voltaje, UPS).
Organización	Falta de procedimientos para el registro/retiro de usuarios.
	Ausencia de protocolos para la salida de equipos tanto internos como externo
	Ausencia de acuerdos de niveles de servicio (ANS o SLA)

	Ausencia de mecanismos de monitoreo a la seguridad
	Ausencia de políticas para el uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia.

6.3 ANALISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Para el contexto de este plan, el objetivo del análisis de riesgo es el de identificar y valorar los riesgos a los que se encuentran expuestos los flujos de información buscando establecer los controles pertinentes para la seguridad de los activos de información.

En esta etapa se hace necesario establecer los criterios bajo los cuales se evaluarán la importancia de los riesgos de seguridad y privacidad de la información, estos criterios serán revisados de manera permanente, considerando los cambios que se den en la institución. Para la definición de los criterios se deberán tener en cuenta lo siguiente:

- La naturaleza, los tipos de causa.
- La naturaleza, los tipos de causa y las consecuencias que puedan tener y como se van a medir.
- La manera en la que se definirán la probabilidad de ocurrencia de un evento.
- La manera en la que se determinará el nivel de riesgo.
- Los niveles de riesgo aceptables para la organización.

En este sentido, para la identificación de amenazas y vulnerabilidades y riesgos, se tienen en cuenta los resultados de las entrevistas con los dueños o responsables de cada proceso implicado además del análisis de riesgo existente. Con el fin de establecer los niveles de riesgo a los cuales se encuentran expuestos los procesos implicados, se realiza la medición de la probabilidad de ocurrencia de las amenazas y el posible impacto que tendrían las consecuencias de su materialización. Por tanto, se establece la probabilidad de ocurrencia para cada riesgo de acuerdo con la siguiente escala:

VALORACIÓN ASIGNADA	VALOR ASIGNADO	FRECUENCIA
Insignificante	1	Se ha presentado una vez en los últimos tres a cinco años
Bajo	2	Ha ocurrido una vez en los últimos >= tres y < cinco años
Moderado	3	Ha ocurrido >= una vez en el período >= un año y < tres años
Mayor	4	Ha ocurrido entre una y tres veces en el último año
Catastrófico	5	Ha ocurrido más de tres veces en el último año

De igual manera, se determina el impacto de cada riesgo de acuerdo con la siguiente escala:

VALORACIÓN ASIGNADA	VALOR ASIGNADO	IMPACTO	
		CUANTITATIVO	CUALITATIVO
Insignificante	1	Afectación <= 1% de la población institucional	Sin afectación de la integridad.
		No hay afectación medioambiental	Sin afectación de la disponibilidad.
		No hay afectación a la divulgación / no hay fuga de información	Sin afectación de la confidencialidad
Bajo	2	Afectación <= 2% de la población institucional	Afectación leve de la integridad.
		Afectación <=1% del presupuesto anual de la entidad.	Afectación leve de la disponibilidad.
		Afectación leve del medio ambiente requiere de 1 semanas de recuperación.	Afectación leve de la confidencialidad.
Moderado	3	Afectación <=5% de la población institucional	Afectación moderada de la integridad de la
			información debido al interés particular de los empleados y terceros.
		Afectación <=3% del presupuesto anual de la entidad.	Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros.
		Afectación leve del medio ambiente requiere de 3 semanas de recuperación.	Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Mayor	4	Afectación <=10% de la población institucional	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros.
		Afectación <=5% del presupuesto anual de la entidad.	Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.
		Afectación importante del medio ambiente que requiere de <=2 meses de recuperación.	Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
Catastrófico	5	Afectación <=30% de la población institucional	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros.
		Afectación <=10% del presupuesto anual de la entidad.	Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.
		Afectación muy grave del medio ambiente que requiere de <=2 años de recuperación.	Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Nota: es preciso destacar que la probabilidad y el impacto se determinan con base en las amenazas y no en las vulnerabilidades.

Nota: es preciso destacar que la probabilidad y el impacto se determinan con base en las amenazas y no en las vulnerabilidades.

6.4 EVALUACIÓN DE CONTROLES PARA LA MITIGACIÓN DE LOS RIESGOS

La evaluación de los controles se realiza una vez se ha definido el riesgo inherente para los

procesos, el impacto y la probabilidad de ocurrencia de cada uno de los riesgos establecidos. Esta evaluación se realiza identificando cada uno de los criterios relacionados a cada uno de los riesgos definidos.

CARACTERÍSTICA	DESCRIPCIÓN
Naturaleza del Control	Establece si el control es manual, mixto o automático
Documentación	Detalla si el control está documentado (si) / no está documentado (no)
Evidencia	Expresa si el control está Divulgado o no divulgado
Tipo de control	Detalla si el Control es: detectivo, preventivo o correctivo

Siendo, así las cosas, para cada tipo de control definido, se presentan los siguientes porcentajes para definir su eficacia:

TIPO DE CONTROL	PORCENTAJE
Manual, mixto o automático	25%
Documentado (si) / no está documentado (no)	25%
Detectivo, preventivo o correctivo	25%
Divulgado o no divulgado	25%

Bajo este escenario, la cobertura efectiva del control permite identificar en que porcentaje se está mitigando el control, para lo cual se definen los siguientes pesos para el nivel de cobertura:

NIVEL DE COBERTURA	PESO
Más del 90%	10
Entre 80 y 90%	9
Entre 70 y 80%	8
Entre 60 y 70%	7
Entre 50 y 60%	6
Entre 40 y 50%	5
Entre 30 y 40%	4
Entre 20 y 30%	3
Entre 10 y 20%	2

6.5 TRATAMIENTO DE RIESGOS.

Teniendo en cuenta los resultados obtenidos en el análisis de riesgos y buscando el adecuado tratamiento al riesgo residual, es preciso declarar los niveles de riesgo y llevar a cabo las acciones de mejora pertinentes, para conservar los principios de confidencialidad, integridad y disponibilidad de los activos de información.

NIVELES DE RIESGO			
TIPO DE RIESGO	VALOR ASIGNADO	ACCIÓN REQUERIDA	GESTIÓN REQUERIDA
Riesgo Catastrófico	Mayor a 12	Requiere acciones inmediatas para evitar lapérdida de la confidencialidad, integridad y disponibilidad de la información	Mitigar
Riesgo Alto	>8 y <= 10	Requiere de acciones rápidas por parte de la Alta Dirección para disminuir el riesgo.	Mitigar
Riesgo Moderado	>5 y <= 8	Se requiere seguir ejecutando los controles definidos para el riesgo y revisar eficacia de estos.	Mitigar
Riesgo Bajo	>= 2 y <=4	El riesgo se mitiga con actividades propias y por medio de acciones detectivas y preventivas.	Aceptar
Riesgo insignificante	1	El riesgo no representa Impacto significativo para la Entidad	Aceptar

Según ISO 31000:2018 las opciones para el tratamiento de riesgos no son excluyentes

- entre sí, y mucho menos resultan eficaces en todas las circunstancias. Por lo tanto, dentro de las acciones que se pueden incluir tenemos:
- Eliminar el riesgo.
- Asumir el riesgo.
- Tomar Acciones para disminuir la probabilidad de ocurrencia del riesgo.
- Implementar acciones para mitigar el riesgo.
- Compartir el riesgo.
- Retener el riesgo.

Así mismo, es preciso que se tengan en cuenta los siguientes factores para el establecimiento del tratamiento del respectivo riesgo:

- Si este se encuentra en una zona de aceptación o apetito de riesgo.
- Todos los riesgos que se encuentren en un nivel de exposición alto o extremo deben recibir el respectivo tratamiento.

6.6 SEGUMIENTO Y REVISIÓN DEL PROCESO PARA LA GESTIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

Este es uno de los aspectos más relevantes del proceso de gestión del riesgo, en las que los roles, responsabilidades del seguimiento, monitoreo y evaluación deben estar claramente establecidos y abarcar todos los aspectos del proceso de gestión del riesgo. Es así como el responsable de llevar a cabo este proceso es el director de TI de la IES INFOTEP, en coordinación con el jefe de planeación y el líder de calidad. Dentro de las actividades que deben llevarse a cabo en esta etapa encontramos:

- Analizar los cambios, las tendencias, lo éxitos y fracasos dentro del proceso de gestión de riesgo de la seguridad de la información.
- Detectar los cambios en el entorno tanto interno como externo.
- Revisar la implementación de los planes para el tratamiento de los riesgos de seguridad de la información.

- Identificar nuevos riesgos de seguridad y privacidad de la información.
- Los procesos para la revisión de los riesgos deben hacerse por lo menos una vez al año, y debe ser continuo y permanente por parte de los lideres de cada proceso.

6 DEFINICIONES Y TERMINOS

- **Activos de información**: en el ámbito de la seguridad de la información pueden definirse como aquellos elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Aceptación de riesgo:** Decisión Institucional de asumir un riesgo
- **Amenazas:** se considera como una situación potencial de materialización de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Análisis de Riesgo**: Uso sistemático de la información para identificar fuentes y estimar el riesgo (Guía ISO/IEC 73:2002).
- **Apetito al riesgo:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.
- Confidencialidad: es la propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **Evaluación del riesgo:** Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
- **Factor de riesgo**: Agente ya sea humano o tecnológico que genera el riesgo.
- **Gestión del riesgo:** proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento

razonable con respecto al logro de los objetivos.

- **Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** propiedad de exactitud y completitud.
- **Riesgo**: Efecto de la incertidumbre sobre el cumplimiento de los objetivos.
- **Riesgo de seguridad digital:** combinación entre amenazas y vulnerabilidades en el entorno digital.
- **Riesgo Inherente:** Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
- **Riesgo residual:** Nivel restante de riesgo después del tratamiento del riesgo.
- **Tratamiento del riesgo:** Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.
- **Vulnerabilidad:** La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.