INSTRUCTIVO PARA LA IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y VALORACIÓN DE CONTROLES EXISTENTES

Septiembre 2024

OBJETIVO

Direccionar a las diferentes dependencias de la Agencia Nacional de Tierras (ANT), en el procedimiento para la identificación y valoración de riesgos de seguridad de la información, así como en la verificación de los controles existentes bajo la ISO 27001:2022, como insumos para la generación de la matriz de riesgos de seguridad de la información.

ALCANCE

La presente Guía aplica a todos los procesos de la ANT para la identificación de riesgos y en paralelo con el Procedimiento para la Administración de Riesgos de Seguridad de la información tiene su alcance desde la comprensión del contexto de la ANT como base para la identificación de los Riesgos de seguridad de la información, hasta la evaluación de la efectividad del tratamiento de riesgo establecido.

DEFINICIONES

Acciones: Mecanismos o estrategias a llevar a cabo para evitar, reducir, asumir o compartir el riesgo.

Activos de información: Según la norma ISO 27001, un activo de información es todo aquello que tiene algún valor para la organización y que, por ende, debe protegerse. Este activo contiene información, ya sea en medios digitales, en papel o en otros medios y pueden ser tangibles o intangibles.

Amenaza: Es una acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

Análisis de Riesgos: Establecimiento de la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.

Causas: Medios, circunstancias, factores o agentes que pueden generar la materialización el riesgo.

Calificación del riesgo: Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

Contexto de la organización: Cuestiones internas y externas de la Agencia Nacional de Tierras, tanto de carácter social, económico, cultural, de orden público, político, legal y cambios tecnológicos, entre otros.

Consecuencias: Efectos o situaciones resultantes de la materialización del riesgo que impactan, en alguna medida, en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Mecanismos o estrategias establecidas para disminuir la probabilidad de ocurrencia del riesgo, el impacto de los riesgos y/o asegurar la continuidad del servicio en caso de llegarse a materializar el riesgo.

Control automático: son ejecutados por un sistema.

Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

Control manual: controles que son ejecutados por personas.

Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Descripción: Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Evaluación: Nivel en que se encuentra el riesgo resultado de calificar el riesgo con base a la probabilidad y el impacto de ellos.

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias (Evento= es un riesgo materializado).

Impacto: Consecuencias pueden afectar al proceso o a la entidad si se llega a materializar el riesgo.

Integridad: Propiedad de exactitud y completitud.

Mapa de riesgos: documento con la información resultante de la administración del riesgo.

Política para la gestión de riesgos y oportunidades: Declaración de la Dirección general de sus intenciones globales con respecto a los Riesgos y Oportunidades.

Probabilidad: Posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de "frecuencia", cuando existen datos verificables de la previa materialización del riesgo en la entidad o con criterios de "factibilidad", cuando se presume que nunca antes se ha materializado el riesgo en la entidad.

Plan de Acciones Preventivas: Conjunto de acciones preventivas dirigidas al fortalecimiento de los controles para la mitigación del riesgo, donde se define la acción, tiempo de ejecución, evidencia y responsable.

Responsables: Dependencias o funcionarios encargados de asegurar la ejecución de las acciones para el tratamiento de los Riesgos.

Riesgos: Efecto de la incertidumbre sobre los objetivos de la Agencia Nacional de Tierras.

Riesgo de Gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgos Estratégicos: Afectan el cumplimiento de los objetivos del Plan Estratégico de la Agencia Nacional de Tierras.

Riesgos Inherente: Riesgo permanente que no se puede separar de una actividad o de un proceso, por formar parte de su naturaleza. Se considera riesgo inherente el que es evaluado sin reconocer y sin valorar el efecto de los controles que ya están establecidos en los procesos y procedimientos de la entidad.

Riesgos Residual: Nivel de riesgo que permanece luego de reconocer y valorar el efecto que los controles, ya establecidos en la entidad, tienen sobre el nivel de riesgo inherente.

Riesgo de Seguridad de la Información: 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)

Tolerancia al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes.

Valoración: Resultado de confrontar el riesgo con la calidad de los controles existentes.

Vulnerabilidad: Se trata de una debilidad o fallo en un sistema de información que abre la puerta para que un atacante o situación no prevista pueda comprometer la integridad, disponibilidad o confidencialidad de los datos.

DOCUMENTOS ASOCIADOS

- DEST-Política-001 ADMINISTRACIÓN DEL RIESGO
- DEST–P-011 Procedimiento de Administración De Riesgos De Seguridad De La Información
- INTI-Política-001 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- DEST-F-004 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
- ANEXO 1 - SOLICITUD DE MODIFICACIONES AL MAPA DE RIESGOS DE GESTIÓN
- ANEXO 2 - REPORTE DE MATERIALIZACIÓN DE RIESGOS
- ANEXO 3 - REPORTE DESEMPEÑO ACCIONES PREVENTIVAS
- GINFO-P-011 PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
- GINFO-F-028-Registro de Incidentes de Seguridad de la Información

Como lo establece la Guía de administración del riesgo de función pública, se debe tener en cuenta que la política de seguridad digital se vincula al 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 habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

Por lo anterior, en lo relacionado a la gestión de los riesgos de seguridad de la información se tendrán como soporte las disposiciones de la "GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS" Versión 6 y la articulación de la misma con la norma ISO 27001:2022

Para iniciar el procedimiento de identificación y valoración de riesgos de seguridad de la información en la ANT, se deberá tener en cuenta que el desarrollo e implementación del mismo consistirá en un trabajo articulado entre las dependencias y la Subdirección de sistemas de información, es decir, que habrá un acompañamiento permanente por parte de la SSIT desde el análisis del contexto de cada proceso, pasando por la identificación y valoración de riesgos, la verificación de los controles existentes, hasta el establecimiento de acciones y formulación del plan de tratamiento de riesgos.

Cada dependencia deberá tener en cuenta para el inicio de este proceso, hacer una contextualización de la entidad, entiendo esto como la revisión de la articulación de las acciones a cargo con elementos como:

- Misión y Visión de la ANT
- Objetivos estratégicos
- Plan Nacional de Desarrollo
- Mapa de proceso y caracterizaciones
- Política de administración de riesgos de la ANT.

ACTIVIDADES

1. Planificar y alistar los insumos necesarios para la identificación de riegos

Teniendo en cuenta el DEST–P-011 Procedimiento Administración De Riesgos De Seguridad De La Información y posterior a la actualización y elaboración del inventario de activos de información mediante la aplicación de los criterios de confidencialidad, disponibilidad e integridad:

Criterios de Confidencialidad

CONFIDENCIALIDAD		
1) PÚBLICO EN GENERAL	PÚBLICA	BAJO
2) INTERNO DE LA ENTIDAD	GENERAL (uso interno)	MEDIO
3) PROCESOS	CLASIFICADA	ALTO
4) ALTA DIRECCIÓN	RESERVADA	ALTO

Criterios de Integridad

INTEGRIDAD		
PREGUNTA	**PUNTAJE**	**Valoración**
Se produce impacto por el compromiso de la integridad del activo de información a nivel:		
1) INSIGNIFICANTE	1	BAJO
2) MENOR	2	BAJO
3) MODERADO	3	MEDIO
4) MAYOR	4	ALTO
5) CATASTRÓFICO	5	ALTO

Criterios de disponibilidad

DISPONIBILIDAD	
PREGUNTA	**PUNTAJE**
La pérdida de disponibilidad:	
1) NO APLICA / NO ES RELEVANTE	0
2) ES CRÍTICO PARA LAS OPERACIONES INTERNAS	0,5
3) PODRÍA AFECTAR LA TOMA DE DECISIONES	1
4) ES CRÍTICO PARA EL SERVICIO HACIA TERCEROS	1,5
5) PUEDE GENERAR INCUMPLIMIENTOS LEGALES Y REGLAMENTARIOS	2

PREGUNTA	PUNTAJE
El tiempo máximo de recuperación aceptable es:	
1) 4 HORAS	2,5
2) 8 HORAS	2,25
3) 24 HORAS	2
4) 48 HORAS	1,5
5) 7 DÍAS	1,25
6) 14 DÍAS	1
7) 30 DÍAS	0,5
8) >30 DÍAS	0,25

DISPONIBILIDAD	
BAJO	Menor que 2
MEDIO	Mayor a 2 y menor que 3,0
ALTO	Mayor a 3,0

De igual forma es importante tener en cuenta la clasificación por tipo de activo:

TIPO DE ACTIVO	DESCRIPCIÓN
INFORMACIÓN	Información vital o estratégica para la ejecución de la misión o los objetivos negocio de la organización. Información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad
HARDWARE	Cualquier componente de hardware que sea necesario para realizar operaciones de almacenamiento o procesamiento de información.
SOFTWARE	Son los correspondientes a todos los programas, aplicaciones que contribuyen al funcionamiento de un conjunto de procesamiento de datos
RED	todos los activos de información, correspondientes a Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro, tales como, interfaz de comunicación, red telefónica, red inalámbrica, telefonía móvil, satelital, red local (LAN), red metropolitana (MAN), internet, radio comunicaciones, punto a punto, ADSL, red digital (rdsi) de la Entidad.
INSTALACIONES	Correspondientes al espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa, también se consideran como infraestructura a otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos, por ejemplo: Fuentes de alimentación, generadores eléctricos, equipos de climatización, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, fibra óptica, equipos de destrucción de soportes de información, mobiliarios, armarios, cajas fuertes, equipos de cómputo de la Entidad.
SERVICIOS	Se relacionan todos los activos de información, correspondientes a la prestación de un servicio por parte de Fonade para el apoyo de las actividades de los procesos, tales como: internet y página web de la Entidad entre otros equipos de cómputo de la Entidad.
PERSONAS	se relacionan todos los activos de información, correspondientes a aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo, usuarios internos y externos, operadores, administradores de sistemas, administradores de comunicaciones, administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores.

Se deberán asegurar y determinar los recursos necesarios como entradas para el desarrollo del procedimiento de administración riesgos de seguridad de la información

a. Inventario de activos de información: Matriz de activos clasificados de acuerdo a los criterios descritos.
b. Inventario de riesgos actuales: Matriz de riesgos de seguridad de la información con la se cuente al inicio del proceso
c. Resultados de seguimientos anteriores: generados por auditorías internas, materialización de riesgos o seguimientos a proceso y controles.

d. Programación de mesas técnicas: Cronograma de reuniones programadas con cada dependencia para la identificación y/o actualización de los riesgos de seguridad de la información.

2. Establecer alcance y contexto

Con el objetivo de identificar y valorar riesgos de seguridad de la información que den respuesta a las necesidades de la ANT y requerimientos de las partes interesadas, la Subdireccion de sistemas de información (SSIT), desarrollará un análisis del contexto interno y externo mediante la implementación de una matriz FODA y una matriz Pestel que permita el análisis de factores como:

Matriz FODA

- Fortalezas: acciones internas de la ANT que permiten la mejora continua de sus procesos y el alcance de objetivos a todos los niveles
- Oportunidades: Factores externos sobre los cuales no se tiene control, pero que mediante el accionar de estrategias a nivel interno permiten el fortalecimiento de la entidad.
- Debilidades: Elementos internos que tiene grandes oportunidades de mejora y que están afectando la entidad
- Amenazas: Factores externos que pueden ocasionar daño a las estrategias de la entidad y por ende al alcance de sus objetivos

Matriz PESTEL

- Político: indican de qué forma las acciones y medidas del gobierno pueden influir en la operatividad y rendimiento de la entidad
- Económico: Variables macroeconómicas que afectan el desempeño de la entidad
- Social y Cultural: aspectos tales como la creencia, cultura, religión, costumbres y preferencias de cada individuo, que puede influir en los procesos de la entidad.
- Tecnológico: Aspectos tecnológicos que, por su contante cambio y actualización, repercuten fácilmente en el contexto de la entidad y en sus procesos.
- Ecológico o ambiental: Factores ambientales que pueden ocasionar cambios el proceso de la entidad
- Legal: normativas y leyes que las entidades están obligadas a cumplir y respetar y que son insumo para el desarrollo de procesos, proyectos y planes.

Una vez elaborados estas herramientas se consolidará la información en el formato establecido por la ANT para los riesgos de seguridad de la información DEST-F-004 Mapa de Riesgos de Seguridad de la Información en la hoja 2-Contexto

De esta forma se asegurará la disponibilidad de los elementos necesarios desde las áreas estratégicas y operativas para la gestión y administración de los riesgos de seguridad de la información, incluyendo entre estos:

*Elementos de planeación estratégica:
Visión, Misión, Plan estratégico, FODA, Pestel, Contexto y Planes de acción.

*Elementos de planificación operativa:
Inventario de activos de información, Mapa de procesos, Objetivos de los procesos y Caracterizaciones de procesos, planes de mejora por proceso.

*Lineamientos para la administración de riesgos en la entidad:

- Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6,
- DEST-Política-001 ADMINISTRACIÓN DEL RIESGO
- DEST–P-011 Procedimiento Administración De Riesgos De Seguridad De La Información
- INTI-Política-001 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- DEST-F-004 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

3. Establecer criterios de evaluación de riesgos

De acuerdo al DEST–P-011 Procedimiento Administración De Riesgos De Seguridad De La Información, se Identificarán los criterios de valoración de riesgos de seguridad de la información, mediante el uso de la forma. DEST-F-004 Mapa de Riesgos de Seguridad de la Información en la hoja 0 – Criterios

4. Identificar el riesgo

La identificación de riesgos de seguridad de la información se realizará mediante la metodología establecida en la forma DEST-F-004 Mapa de Riesgos de Seguridad de la Información, para ello deberá registrase la siguiente información:

a. Nombre del Proceso
b. Activos de información identificados para el proceso
c. Responsable del proceso
d. DESCRIPCIÓN DEL RIESGO: ¿QUÉ PUEDE SUCEDER? (AMENAZA): Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso, se debe tener en cuenta el ANEXO 1- AMENAZAS de este documento.
e. CAUSAS: ¿CÓMO O POR QUÉ PUEDE SUCEDER? (VULNERABILIDAD): Establecer las causas a partir de los factores determinados en el contexto. se debe tener en cuenta el ANEXO 2- VULNERABILIDADES de este documento.
f. ¿CUÁNDO PUEDE SUCEDER?: de acuerdo con el desarrollo del proceso.
g. CONSECUENCIAS: ¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN? Determinar los posibles efectos por la materialización del riesgo
h. DESCRIPCIÓN DEL RIESGO: Para dicha descripción se debe tener en cuenta la siguiente estructura.

Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

De esta forma, se presentan a continuación algunos ejemplos que eventualmente pueden ser tenidos en cuenta como riesgos de seguridad de la información y a los cuales se les deberá aplicar los criterios para su descripción:

Acceso no autorizado o uso inadecuado de la plataforma tecnológica
Fallas en la configuración, operación y mantenimiento de la plataforma tecnológica
Violación intencional o errores en la administración y manipulación de la plataforma tecnológica por parte de los responsables
Ejecución de aplicaciones malware u otro tipo de código malicioso
Fallas en la implementación de controles de seguridad física
Deficiencias en el proceso de copias de seguridad
Falla intencional o errores en la ejecución de creación y administración de roles y privilegios de los usuarios de los servicios tecnológicos
Manipulación intensional de la información procesada en la plataforma tecnológica para favorecer intereses particulares
Pérdida o falta de integridad de la información almacenada en la plataforma tecnológica y Core del negocio
Subutilización de las implementaciones de aplicativos en la plataforma tecnológica
Publicación errada o adulteración de la información publicada en la página web
Indisponibilidad total o parcial de la plataforma tecnológica de la Entidad
Utilización de software no licenciado - autorizado
Daño o malfuncionamiento del hardware o software
Hurto de activos de la plataforma tecnológica (información, equipos de cómputo, comunicaciones, procesamiento, audiovisuales, etc.)
Ejecución de operaciones no autorizadas sobre los sistemas de información de la Entidad
Aceptar o solicitar sobornos, dadivas o beneficios para la utilización indebida o divulgación no autorizada de información confidencial almacenada en la plataforma tecnológica.
Subutilización de las implementaciones de aplicativos en la plataforma tecnológica

Inoportunidad en la atención de requerimientos de actualización, desarrollo, mejora a los sistemas de información o soporte tecnológico
Indisponibilidad o deficiencias en las funcionalidades de los aplicativos
Incluir proyectos en el Plan Estratégico de Tecnologías de la Información, para beneficio propio o de un superior
Fallas en equipamiento eléctrico e infraestructura física en el centro de datos de la ANT.
Afectación parcial o total de los componentes tecnológicos dispuestos en la ANT
Ciberataque dirigido al Portal Web de la agencia
Indisponibilidad del Recurso Humano asignado a la operación de las plataformas tecnológicas.
Declaración de Estado de emergencia, pandemia, calamidad pública, aislamiento preventivo obligatorio o toque de queda en el país o en donde se operen los servicios tecnológicos y vía web de la agencia

5. Valorar el Riesgo inherente

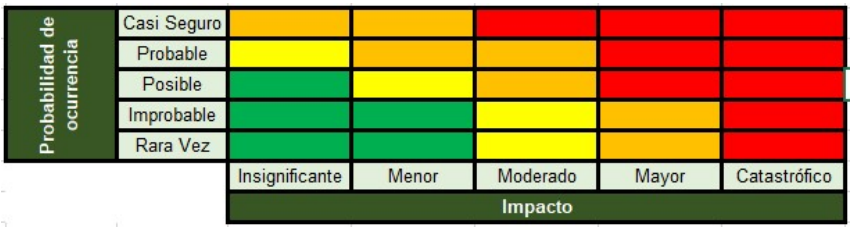
Una vez determinado el proceso, los activos de información asociados, el responsable del proceso y la descripción del riesgo, se procede con la valoración del riesgo en DEST-F-004 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, Hoja 4-VALORACIÓN DEL RIESGO

Se debe establecer el nivel de probabilidad y de impacto de acuerdo a los siguientes criterios:

Valoración de probabilidad de ocurrencia del riesgo			
Nivel	**Descriptor**	**Descripción**	**Frecuencia**
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara Vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Valoración del impacto del riesgo			
Nivel	**Descriptor**	**(CONSECUENCIAS) CUANTITATIVO**	**(CONSECUENCIAS) CUALITATIVO**
5	**Catastrófico**	Afectación =Entre el 100% y el 80% de la población. Afectación =del 50% del presupuesto anual de la entidad o más.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
4	**Mayor**	Afectación =Entre el 79% y el 50% de la población. Afectación =Entre el 49 % y el 20% del presupuesto anual de la entidad.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
3	**Moderado**	Afectación =Entre el 49% y el 20% de la población. Afectación =Entre el 19% y el 10% del presupuesto anual de la entidad.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
2	**Menor**	Afectación =Del 10% de la población o menos. Afectación =9% o menos del presupuesto anual de la entidad.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
1	**Insignificante**	Afectación =no hay afectación de la población. Afectación =No hay afectación del presupuesto anual de la entidad.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.

Seguido a esto se calculará el riesgo inherente mediante el cruce de la probabilidad y el impacto identificados y de acuerdo al siguiente mapa de calor



En donde se tiene en cuenta los siguientes criterios:

De acuerdo a esto y a la tabla de tratamiento del riesgo que se encuentra en el DEST–P-011 Procedimiento Administración De Riesgos De Seguridad De La Información y en esta guía, se determinará la opción de manejo:

TRATAMIENTO	DESCRIPCIÓN	APLICACIÓN
Aceptar	No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado).	Aplicar para riesgos inherentes y residuales en la zona de calificación de riesgo bajo.
Reducir	Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.	Aplica para riesgos residuales moderados, altos y extremos que pueden ser administrado mediante el diseño de nuevos controles o el fortalecimiento de los controles existentes, de modo que en el futuro el riesgo residual se pueda reevaluar como aceptable.
Evitar	Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.	Cuando los escenarios de riesgo identificado se consideran demasiado extremos y las actividades no están establecidas por la ley.
Compartir	Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.	Cuando es muy difícil reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más

		eficacia, generalmente por medio de seguros o de tercerización.

6. Verificar Controles Existentes

-Verificar el diseño de controles teniendo en cuenta: periodicidad, responsable, evidencia, actividad de control al riesgo según ISO 27001:2022.

-Valorar el diseño del control dando respuesta a las siguientes preguntas:

a. RESPONSABLE ¿Existe un responsable asignado a la ejecución del control?
b. RESPONSABLE ¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución de control?
c. PERIODICIDAD ¿La oportunidad en las ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?
d. PROPÓSITO ¿Las actividades que se desarrollan en el control realmente buscan por sí sola prevenir o detectar las causas que pueden dar origen a riesgo?
e. COMO SE REALIZA ¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?
f. QUE PASA CON LAS OBSERVACIONES O DESVIACIONES ¿Las observaciones, desviaciones o diferencias identificadas como resultado de la ejecución del control son investigada y resultas de manera oportuna?
g. EVIDENCIA ¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con l evidencia, llegar a la misma conclusión?

Esta información permitirá la valoración del diseño del control y la valoración de la ejecución del control, bajo los siguientes criterios:

Valoración del DISEÑO del control		
Criterio de evaluación	**Opción de respuesta al criterio de evaluación**	**Peso en la evaluación del diseño del control**
1.1 Asignación del responsable	Asignado	15
	No Asignado	0
1.2 Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un control	0

Valoración del DISEÑO del control		
Criterio de evaluación	**Opción de respuesta al criterio de evaluación**	**Peso en la evaluación del diseño del control**
4. Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
5.Qué pasa con las observaciones o desviaciones	Se investigan oportunamente	15
	No se investigan oportunamente	0
Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0
Fuerte	Si su calificación es entre 96 y 100	
Moderado	Si su calificación es entre 86 y 95	
Débil	si su calificación es entre 0 y 85	

Valoración de la EJECUCIÓN del control	
Rango de calificación de la ejecución	**Peso de la ejecución del control**
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

Una vez realizada esta valoración se deberá valorar la solidez individual del control y la solidez del conjunto de controles, teniendo en cuenta los siguientes criterios:

VALORACIÓN SOLIDEZ INDIVIDUAL DEL CONTROL		
DISEÑO	**EJECUCIÓN**	**SOLIDEZ INDIVIDUAL**
Fuerte	Fuerte	**Fuerte**
Fuerte	Moderado	**Moderado**
Fuerte	Débil	**Débil**
Moderado	Fuerte	**Moderado**
Moderado	Moderado	**Moderado**
Moderado	Débil	**Débil**
Débil	Fuerte	**Débil**
Débil	Moderado	**Débil**
Débil	Débil	**Débil**

VALORACIÓN SOLIDEZ DEL CONJUNTO DE LOS CONTROLES	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50

Finalmente se debe establecer si los controles ayudan a disminuir el riesgo tanto en el factor de probabilidad como de impacto, bajo tres criterios: 1. Directamente, 2. Indirectamente, 3. No disminuye.

Estos valores permiten desplazar las columnas de impacto y de probabilidad, de acuerdo a la siguiente tabla, lo que determinará el riesgo residual y establecerá la opción de manejo de acuerdo a estos criterios: Aceptar, Reducir, Evitar, Compartir:

SOLIDEZ DEL CONJUNTO DE LOS CONTROLES	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR EL IMPACTO	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE PROBABILIDAD	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE IMPACTO
Fuerte	Directamente	Directamente	2	2
Fuerte	Directamente	Indirectamente	2	1
Fuerte	Directamente	No disminuye	2	0
Fuerte	No disminuye	Directamente	0	2
Moderado	Directamente	Directamente	1	1
Moderado	Directamente	Indirectamente	1	0
Moderado	Directamente	No disminuye	1	0
Moderado	No disminuye	Directamente	0	1
Débil	Directamente	Directamente	0	0
Débil	Directamente	Indirectamente	0	0
Débil	Directamente	No disminuye	0	0
Débil	No disminuye	Directamente	0	

7. Elaborar Matriz de riesgos de seguridad de la información

Realizada la identificación y valoración de controles existentes, se debe consolidar la información en la matriz de riesgos, con el objetivo de obtener el mapa de riesgos de seguridad de la información en DEST-F-004 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, Hoja 6-MAPA DE RIESGOS SEGURIDAD

a. Revisar que los valores generados en la hoja 6 MAPA RIESGOS DE SEGURIDAD sean coherentes con la información ya registrada y generada.
b. Definir el indicador del control, en la columna Q.
c. Definir las acciones preventivas que permitan el control y manejo del riesgo, asignando responsable, indicador y fecha de ejecución.

8. Continuidad del procedimiento

Los siguientes pasos del 8 al 21, se desarrollarán de acuerdo al DEST–P-011 Procedimiento Administración De Riesgos De Seguridad De La Información

PARA TENER EN CUENTA…

❖ **Niveles de aceptación del riesgo y tratamiento**

La agencia Nacional de tierras, establece que se realizará identificación de riesgos de seguridad de la información para los activos clasificados en **criticidad alta**, en relación a los activos de información clasificados en criticidad media o baja, se realizará un seguimiento de los mismos durante su vigencia para poder llevar un control de las posibles materializaciones de riesgos sobre estos activos, que pueda llevar a cambiar su nivel de criticidad.

Una vez identificados y valorados los riesgos, la Agencia Nacional de Tierras acepta, solamente, los riesgos residuales en el nivel de exposición de riesgo "Bajo". En estos casos, no será necesaria la formulación del Plan de Acciones Preventivas para el diseño o fortalecimiento de controles. Los riesgos aceptados estarán sujetos a monitoreo por parte de la dependencia responsable del proceso.

En lo correspondiente a las categorías de tratamiento del riesgo y de acuerdo a la DEST-POLITICA-001 Política de administración del riesgo, la Agencia Nacional de Tierras adoptará los lineamientos metodológicos dispuestos por las autoridades administrativas competentes, los cuales serán confirmados según corresponda en el proceso de formulación o modificación al Mapa de Riesgos de seguridad de la información:

TRATAMIENTO	DESCRIPCIÓN	APLICACIÓN
Aceptar	No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado).	Aplicar para riesgos inherentes y residuales en la zona de calificación de riesgo bajo.
Reducir	Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.	Aplica para riesgos residuales moderados, altos y extremos que pueden ser administrado mediante el diseño de nuevos controles o el fortalecimiento de los

TRATAMIENTO	DESCRIPCIÓN	APLICACIÓN
		controles existentes, de modo que en el futuro el riesgo residual se pueda reevaluar como aceptable.
Evitar	Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.	Cuando los escenarios de riesgo identificado se consideran demasiado extremos y las actividades no están establecidas por la ley.
Compartir	Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.	Cuando es muy difícil reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia, generalmente por medio de seguros o de tercerización.

Cabe aclarar que durante este procedimiento se debe entender la materialización del riesgo como la ocurrencia del mismo, es decir que suceda, que la amenaza se materialice dadas las vulnerabilidades existentes, de esta forma, se debe tener en cuenta que para el monitoreo, valoración y reporte de la materialización de los riesgos de seguridad de la información se deberá tener en cuenta los siguientes criterios:

a. Realizar la siguiente operación y determinar el desempeño del control:

$$1 - \left(\frac{\text{\# de enventos}}{\text{Frecuencia del riesgo}} \right)$$

Número de eventos: # de eventos (Evento= es un riesgo materializado)

Frecuencia del riesgo: Número de veces que se realiza la acción (# de veces que se realiza la acción)

b. Proceder con alguna de las siguientes opciones:
   - Si el valor del resultado se encuentra entre el 100% y 90%, no se revisa el control - (Se mantiene)
   - Si el valor del resultado se encuentra entre el 90% y 80%, es potestad de la dependencia revisar el control - (Revisión de control)
   - Si el valor del resultado es inferior al 80%, se debe revisar el control para realizar ajustes (Cambio).

❖ **¿Cómo lograr la efectividad de este proceso?**

Con el objetivo de lograr la efectividad y eficacia de este proceso, será clave dentro del desarrollo del DEST–P-011 Procedimiento Administración De Riesgos De Seguridad De La Información y el uso de la presente Guía las siguientes acciones:

- En caso de presentarse cambios en los procedimientos o procesos a cargo, las dependencias deberán informar a la Subdirección de sistemas de información, dichos cambios.
- Si se adquiere en alguna dependencia, herramientas o se hace uso de nuevas plataformas tecnológicas, debe notificarse a la SSIT.
- Si se genera un nuevo activo de información que se considere importante y pueda ser afectado por falta de confidencialidad, integridad o disponibilidad, deberá ser reportado a la SSIT.
- Se debe mantener la integridad y disponibilidad de las evidencias de la ejecución de controles de seguridad de la información que cada dependencia ejecute.
- Se debe mantener la integridad y disponibilidad de las evidencias de la ejecución de las acciones preventivas establecidas para los riesgos de seguridad de la información en cada dependencia.

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
19/09/2024	01	Creación del documento.

Elaboró: Johanna Rincón Molina	**Revisó:** Andrea Linney Sierra Ladino	**Aprobó:** Diana Lucia Herrera Riaño
Cargo: Contratista	**Cargo:** Contratista	**Cargo**: Subdirectora Sistemas de información de tierras
Firma: ORIGINAL FIRMADO	**Firma:** ORIGINAL FIRMADO	**Firma:** ORIGINAL FIRMADO

ANEXO 1 - AMENAZAS

El presente anexo expone como herramienta a esta guía los ejemplos más comunes de amenazas dentro del procedimiento de identificación y valoración de riesgo de seguridad de la información, las mismas son parte integral de la – ISO/IEC 27005.

En relación al origen las amenazas se clasifican en: Deliberadas (D), fortuitas (F) o ambientales (A).

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D

	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Es importante tener en cuenta algunas amenazas de origen humano

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto	· Piratería
	Ego	· Ingeniería Social
	Rebelion	· Intrusión, accesos forzados al sistema
	Estatus	· Acceso no autorizado
	Dinero	
Criminal de la computación	Destrucción de la información	· Crimen por computador
	Divulgación ilegal de la información	· Acto fraudulento
	Ganancia monetaria	· Soborno de la información
	Alteración no autorizada de los datos	· Suplantación de identidad
		· Intrusión en el sistema
Terrorismo	Chantaje	· Bomba/Terrorismo
	Destrucción	· Guerra de la información

	Explotación	· Ataques contra el sistema DDoS
	Venganza	· Penetración en el sistema
	Ganancia política de los medios de comunicación	· Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva	· Ventaja de defensa
	Espionaje económico	· Ventaja política
		· Explotación económica
		· 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	· Asalto a un empleado
	Ego	· Chantaje
	Inteligencia	· Observar información reservada
	Ganancia monetaria	· Uso inadecuado del computador
	Venganza	· Fraude y hurto
	Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	· 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.

ANEXO 2 - VULNERABILIDADES

El presente anexo expone como herramienta a esta guía los ejemplos más comunes de vulnerabilidades dentro del procedimiento de identificación y valoración de riesgo de seguridad de la información, las mismas son parte integral de la – ISO/IEC 27005.

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable

	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)