Manual de usuario

GESTION DE RIESGOS DE SEGURIDAD DIGITAL - GRC NOVASEC

Proceso: Información, Innovación y Tecnología
Subproceso: Seguridad de la Información
Versión: 02
Código: MN-IIT-0075
Año: 2023

TABLA DE CONTENIDO

Tabla de ilustraciones

1 Objetivo

Establecer las acciones que se deben ejecutar en la herramienta GRC de NOVASEC, para el registro de la gestión de los riesgos de seguridad de la información (la cual incluye los riesgos de protección de datos personales, ciberseguridad, seguridad en nube y analítica de datos), con el fin de facilitar las actividades de identificación, análisis, valoración, tratamiento y monitoreo de la U.A.E. DIAN.

2 Responsables de la gestión de riesgos de seguridad de la información en GRC

La gestión de riesgos de seguridad de la información es responsabilidad de los dueños de los activos de información (primera línea de defensa), quienes deben realizar la implementación de esta metodología, sin embargo, se ha establecido el rol de “enlace de seguridad” quien será el encargado del registro de los diferentes aspectos de la gestión de riesgos de seguridad de la información, en la herramienta GRC de NOVASEC.

La Oficina de Seguridad de la Información estará atenta a cualquier situación o soporte que se requiera, en el caso que el enlace de seguridad no se pueda dar solución.

3 Contenido

3.1 Generar el listado de los activos de información

Se deben seleccionar los activos de información objeto de la gestión de riesgos de seguridad de la información teniendo en cuenta el numeral *3.10.2. Activos de información objeto de la gestión de riesgos de seguridad de la información*, del documento *CT-IIT-0132 Gestión de Riesgos de Seguridad de la Información*.

Para obtener la lista de activos de información de “Alta Criticidad” se debe realizar los siguientes pasos:

a) Ingresar a la herramienta GRC, disponible en: https://grc.dian.gov.co/novasecMS/ y ejecutar la autenticación mediante el usuario y la contraseña (asignado por la Oficina de Seguridad de la Información) y superar la verificación de robots:

Ilustración 1. Ingreso a la herramienta GRC

b) En la pantalla principal del GRC se muestra información general del usuario con los nombres completos, el proceso y la información que puede gestionar:

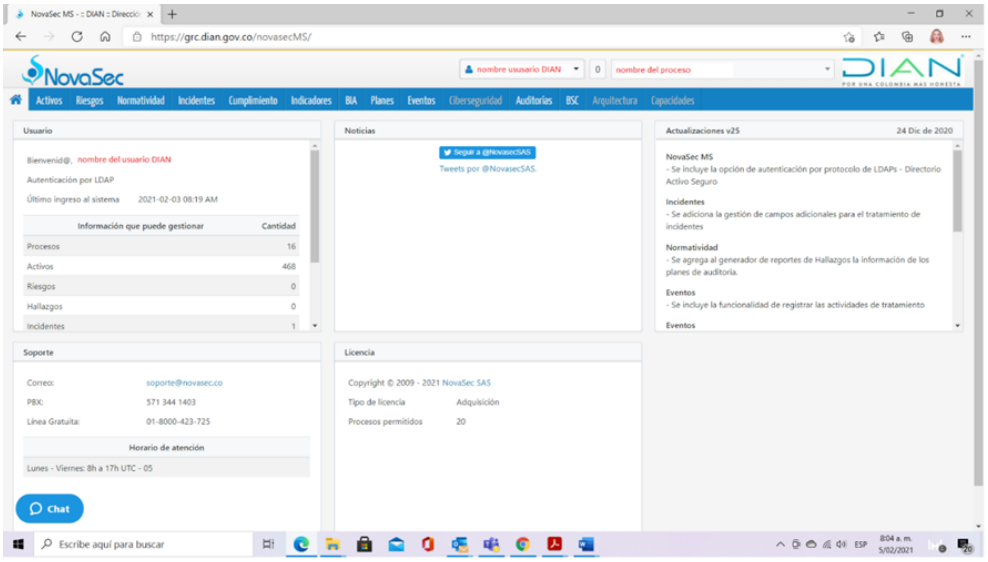


Ilustración 2. Pantalla principal GRC

c) Ingresar al módulo de Activos, seleccionando la opción “Activos” en el menú horizontal superior:

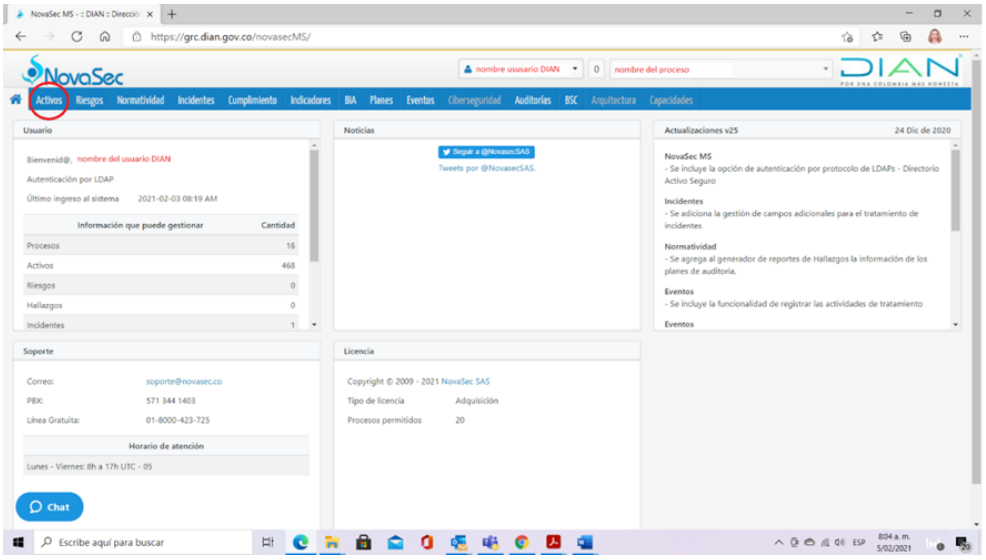


Ilustración 3. Menú activos

d) Al ingresar al Módulo de Activos aparece la siguiente pantalla, en la que debe dar clic a la opción de “Reportes”:

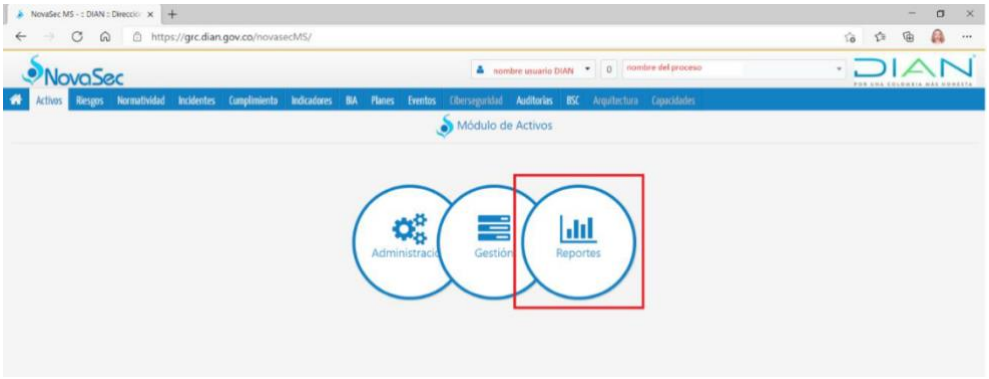


Ilustración 4. Selección menú reportes

e) En el menú vertical Reporte de Activos, escoger la opción “Generador de reportes”:

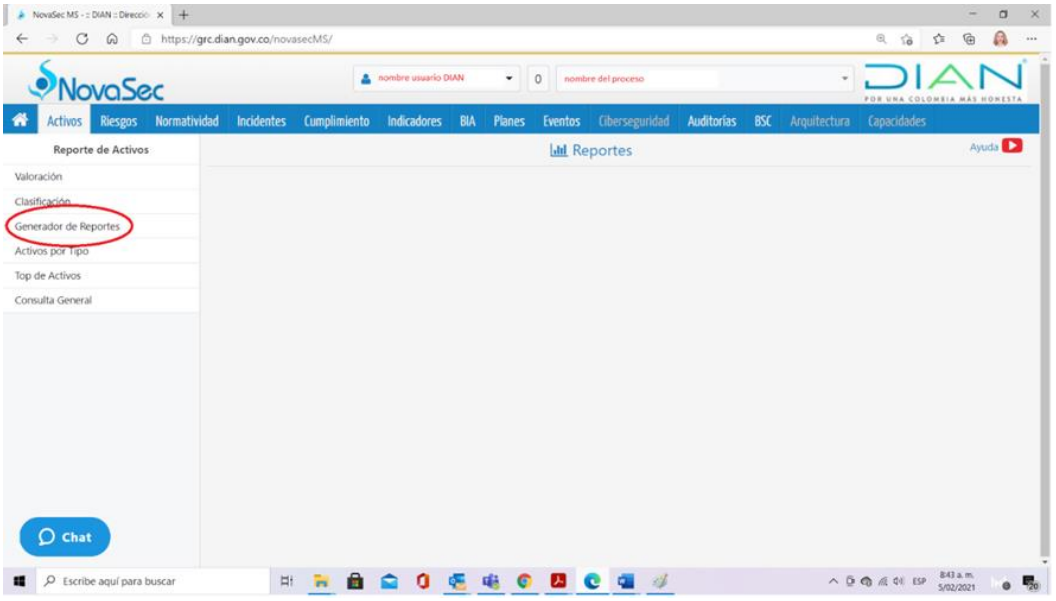


Ilustración 5. Menú generador reportes

f) Se debe seleccionar la opción “agregar” como se muestra a continuación:

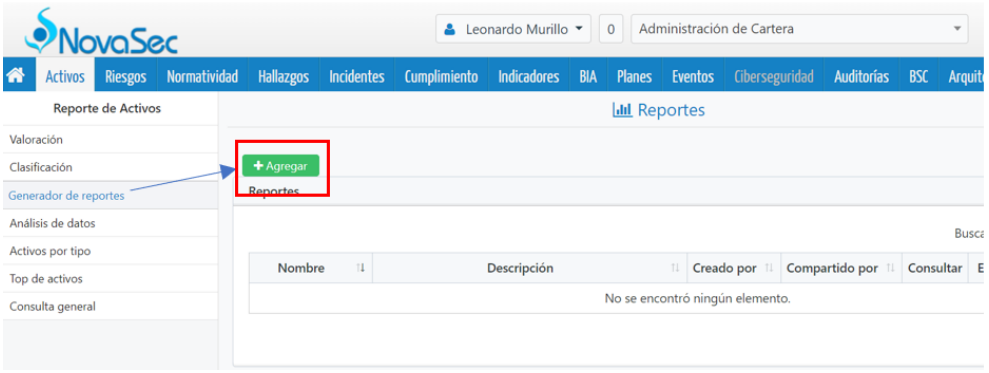


Ilustración 6. Selección botón “aceptar”, menú “reportes

g) Seguido de ello se deben escoger los siguientes valores que se incluirán en el reporte:

- **Nombre del reporte**: El sistema permitirá seleccionar esta información al usuario. Se sugiere incluir el nombre “Análisis de Riesgos para el proceso + **nombre del proceso”**.
- **Descripción**: Activos de alta criticidad para el análisis de riesgos del proceso **nombre del proceso**.
- **Tipo de reporte**: Datos.
- **Macroprocesos**: Se pueden pasar todos los elementos de la izquierda a la derecha, dando clic en el botón , sin embargo se puede seleccionar solo el proceso al que se pertenezca.
- **Procesos**: Se pueden pasar todos los elementos de la izquierda a la derecha, dando clic en el botón , sin embargo se puede seleccionar solo el proceso al que se pertenezca.

h) Una vez diligenciados los campos anteriores, el sistema le permitirá al usuario visualizar los diferentes campos incluidos en la identificación de activos de información, sin embargo, se deben seleccionar los siguientes campos que ayudarán en la gestión de riesgos de seguridad de la información:

- Tipo
- Custodios
- Propietarios
- Valoración
- Confidencialidad
- Integridad
- Disponibilidad
- Infraestructura Crítica Cibernética - Es un ciberactivo:
- Infraestructura Crítica Cibernética - Impacto del ciberactivo
- Clasificación de la Información - Cuenta con datos personales
- Autenticación digital - Autenticación digital

i) Dar clic en el botón  para pasar los campos escogidos del panel de la izquierda al panel de la derecha:

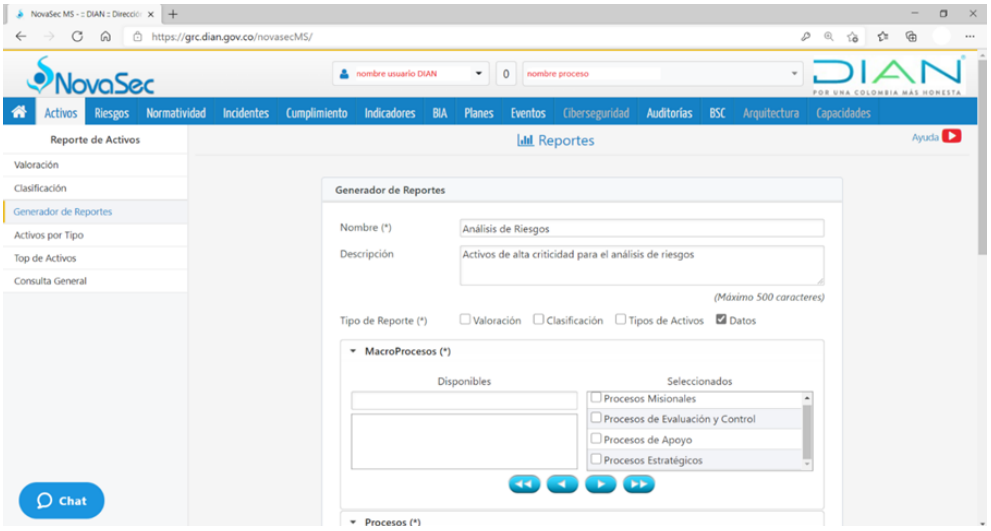


Ilustración 7. Opción de selección de procesos

j) El sistema se encuentra en la capacidad de seleccionar los campos previamente sugeridos, con el valor agregado de poder indicar los criterios que se desean incluir en el informe. Para realizarlo, se debe dar clic en el botón “+ Agregar Criterio”

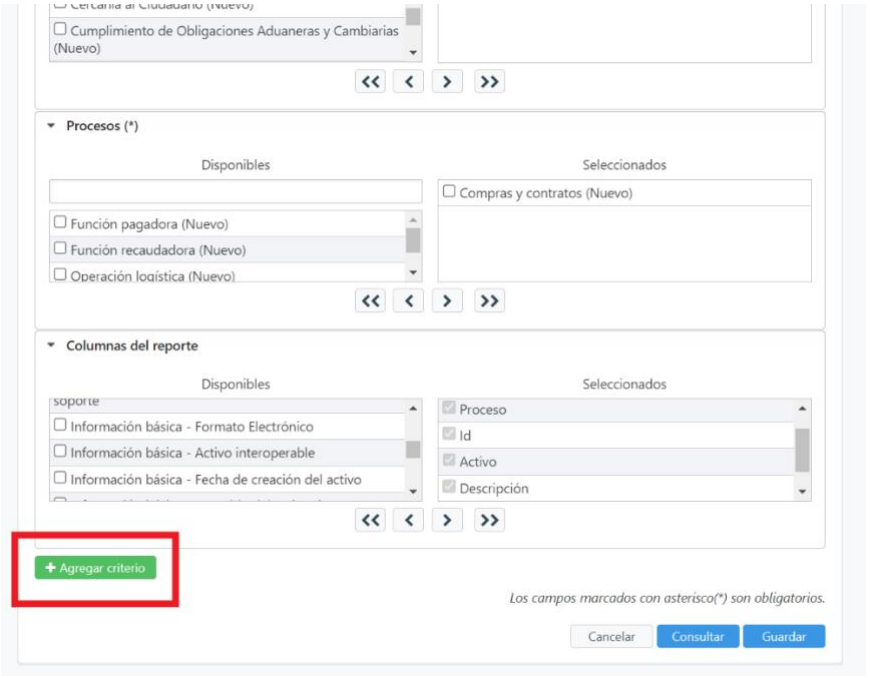


Ilustración 8. Opción agregar criterio

k) El sistema permitirá visualizar todos los campos incluidos en la gestión de activos de información, se debe seleccionar el campo y el criterio que debe considerar como se muestra a continuación:

l)

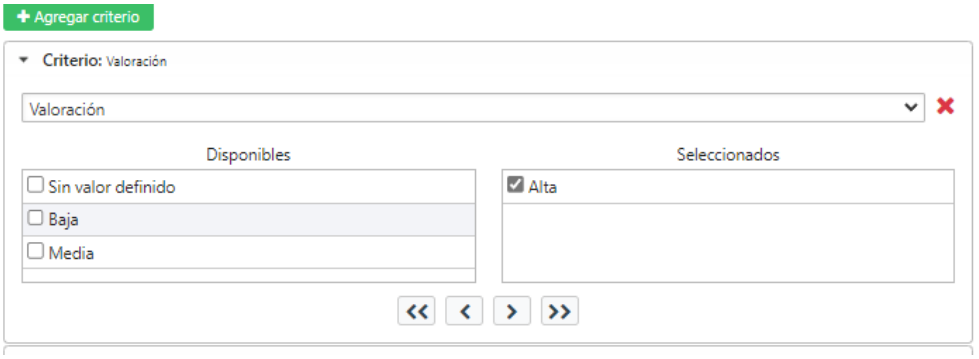


Ilustración 9. Configuración del criterio

m) Una vez seleccionado el criterio se debe trasladar a la parte derecha de la pantalla seleccionado el botón ›. Se pueden incluir cuantos criterios se deseen de la lista desplegable

n) Dar clic en el botón “Guardar”. En la pantalla aparecen todos los reportes que se hayan generado.

o) Escoger el reporte recién creado y dar clic en “Consultar” como se muestra a continuación:

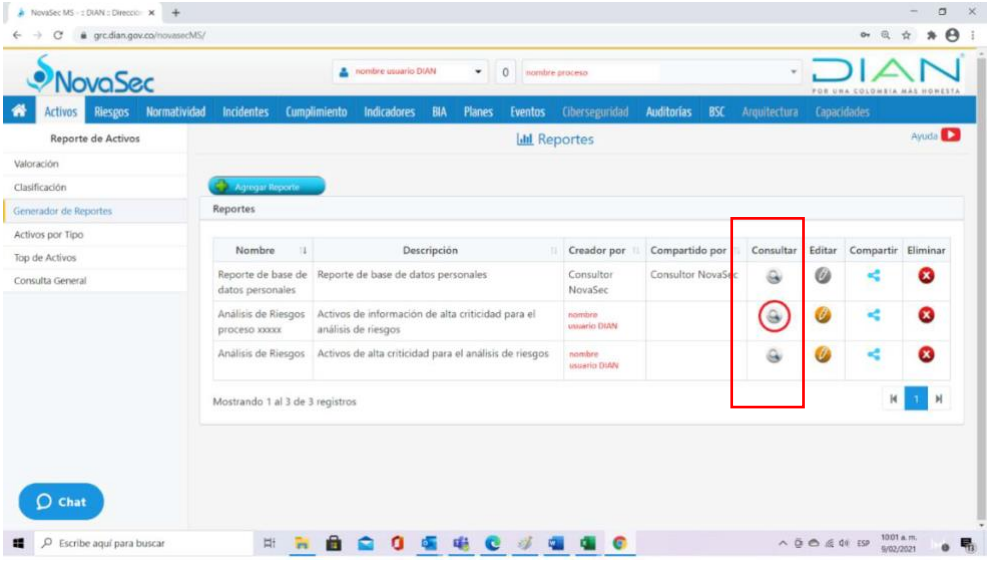


Ilustración 10. Consulta de reportes

p) Como resultado se pueden ver en la pantalla los activos de información seleccionados para el análisis de riesgos. Esta consulta también se puede generar en un archivo Excel, dando clic en el ícono .

q) El sistema le permitirá visualizar la siguiente imagen:

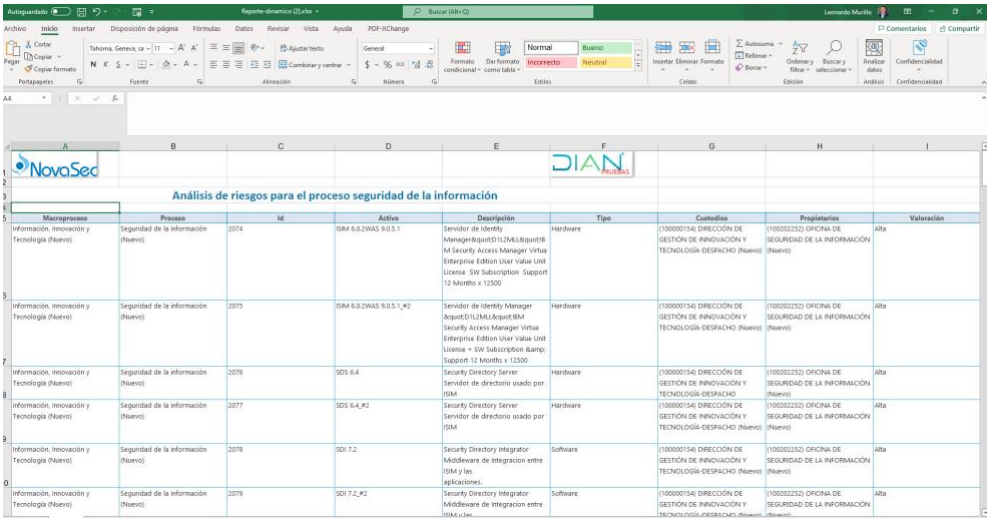


Ilustración 11. Reporte generado en Excel

r) Ubicados en el Excel el usuario deberá filtrar las columnas para identificar activos de información con las siguientes características:

- **Activos de información con valoración "Alta"**
- **Activos considerados Infraestructura Crítica Cibernética-ICC**
- **Activos con Datos Personales**
- **Activos relacionados con autenticación digital**
- **Activos con valoración con Disponibilidad "Alta**

Nota: para más información por favor consultar el documento CT-IIT-0132 Gestión de riesgos de seguridad de la información en el numeral *3.10.2 Activos de información objeto de la gestión de riesgos de seguridad de la información*

3.2 Registro de riesgos de seguridad de la información

Nota: previamente se configuró en el sistema los controles transversales, amenazas, vulnerabilidades, y el usuario debe buscar las vulnerabilidades y amenazas que consoliden el riesgo para el activo de información que se está evaluando. Para más detalle se debe consultar las *tablas de vulnerabilidades, amenazas, controles y riesgos tipo* en el *Instrumento de consulta para la gestión de riesgos de seguridad de la información.*

3.2.1 Instrumento de consulta para la gestión de riesgos de seguridad de la información

A continuación se da una explicación del contenido de este documento el cual se encuentra publicado en la DIANNET:

- **Tabla de vulnerabilidades:** incluye las vulnerabilidades transversales que se han identificado dependiendo el tipo de activo de información que se encuentra identificado en la entidad:

Id	Vulnerabilidad	Principio			Medio de conservación		Tipo de activo relacionado
		C	I	D	Físico	Electrónico	
V1	Conexiones a red pública desprotegidas	X		X		X	Servicio

Ilustración 12. Campos tabla de vulnerabilidades

Los campos de esta tabla son los siguientes:

a. **Id:** Identificador de la vulnerabilidad en el sistema
b. **Vulnerabilidad:** nombre asignado de la vulnerabilidad
c. **Principio:** principio al cual puede afectar la vulnerabilidad entre Confidencialidad, Integridad y Disponibilidad
d. **Medio de Conservación:** identifica si la vulnerabilidad pueda afectar un activo de información físico o Electrónico
e. **Tipo de Activo relacionado:** identifica a qué tipo de activo de información puede afectar la vulnerabilidad dadas sus características y comportamiento

- **Tabla de amenazas:** incluye las amenazas identificadas que puede afectar a una determinada vulnerabilidad identificada dentro de la organización, dado que como premisa “la existencia de una vulnerabilidad por sí sola no se categoriza como un riesgo, para la existencia de este debe existir una amenaza que pueda explotarla”

id	Nombre Amenaza	Descripción Amenaza	Causa de la amenaza: AI: Ataques Intencionados DN: Desastres Naturales DOI: De Origen Industrial EFNI: Errores y Fallos No Intencionados ADP: Afectación Datos Personales CI: Ciberseguridad	Vulnerabilidades Asociadas
A1	Suplantación de identidad de los usuarios	El atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la DIAN o por personal contratado temporalmente. Se conoce también como usurpación de derechos. Hurto o robo de identidad digital (DI-269I)	AI	(V8,V27,V28,V42,V46,V48,V50,V54, V55,V64,V68,V75, V98, V174)

Ilustración 13. Campos tabla de amenazas

Los campos de esta tabla son los siguientes:

a. **Id:** Identificador de la amenaza en el sistema
b. **Nombre amenaza:** nombre asignado a la amenaza
c. **Descripción amenaza:** establece un resumen de las principales características de la amenaza
d. **Causa de la amenaza:** identifica cual es la causa que puede generar la amenaza
e. **Vulnerabilidades asociadas: i**dentifica las vulnerabilidades que pueden verse afectadas por esta amenaza, de igual manera se puede buscar en la tabla de vulnerabilidades toda la información asociada a la vulnerabilidad.

- **Tabla de controles:** identifica los controles tomados de buenas prácticas internacionales que se deben aplicar a una determinada vulnerabilidad para mitigar/reducir el riesgo identificado.

Numeral	Nombre del control	Descripción Control	Vulnerabilidades	Tipo de Control	Control ISO 27001:2013	Controles necesarios en la gestión de proyectos		Justificación de la inclusión/ exclusión
Anexo A – NTC-ISO/IEC 27001:2022						Necesario		
5.	Controles Organizacionales					SÍ	No	
5.1	Políticas de seguridad de la información	La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios	V24, V25,V32,V34,V35, V41,V44,V46,V55,V93	Preventivo	05.1.1 05.1.2		X	

Ilustración 14. Campos tabla de controles

Los campos de esta tabla son los siguientes:

a. **Numeral:** identificador del control en el sistema
b. **Nombre del control:** nombre asignado al control
c. **Descripción control:** establece un resumen de las principales características del control
d. **Vulnerabilidades:** identifica las vulnerabilidades que pueden mitigar/reducir la aplicación del control
e. **Tipo de Control:** identifica si el control es preventivo / detectivo (el cual mitiga la probabilidad de ocurrencia) o correctivo (el cual mitiga el impacto)
f. **Control ISO 27001:2013:** identifica la relación del control identificado con la norma ISO 27001:2013

- **Tabla de riesgos tipo:** consolida la información de las amenazas, vulnerabilidades y controles asociados, para brindar una herramienta de consulta a los responsables de la gestión de los riesgos de seguridad de la información

ID Vulnerabilidad	Vulnerabilidad	Tipo de activo	Tipo de Riesgo	Descripción del Riesgo	Id Amenazas	Amenazas	Controles asociados	Descripción del control
V2	Inadecuada o insuficiente protección del tráfico sensible	Servicio	Pérdida de confidencialidad Pérdida de disponibilidad	Inadecuada o insuficiente protección del tráfico sensible pueden causar Falla de servicios de comunicaciones, Realización de Hackeo no ético, Afectación por errores de secuencia, Afectación por el análisis de tráfico en las comunicaciones, Iterceptación o interrupción de canales encubiertos y tráfico clandestino. causando pérdida de confidencialidad, disponibilidad.	A17, A24, A41, A65, A82	Falla de servicios de comunicaciones, Realización de Hackeo no ético, Afectación por errores de secuencia, Afectación por el análisis de tráfico en las comunicaciones, Iterceptación o interrupción de canales encubiertos y tráfico clandestino.	5.1	Políticas de seguridad de la información

Ilustración 15. Campos tabla riesgos tipo

Los campos de esta tabla son los siguientes:

a. **Id vulnerabilidad:** identifica la vulnerabilidad que se está analizando
b. **Vulnerabilidad:** nombre de la vulnerabilidad
c. **Tipo de activo:** identifica el tipo de activo que este asociado a la vulnerabilidad
d. **Tipo de riesgo: i**dentifica el tipo de riesgos que afecta la vulnerabilidad bien sea Confidencialidad, Integridad y/o Disponibilidad

   Nota: el usuario para este campo debe registrar un tipo de riesgo a la vez, y no se debe registrar 2 o más tipos de riesgos de manera simultánea, sin importar si cuentan con las mismas amenazas o vulnerabilidades.

e. **Descripción del riesgo:** detalla la vulnerabilidad que se identifica la amenazas que se identifica afecta a dicha vulnerabilidad y los principios de seguridad de la información que puede afectar
f. **Id Amenazas:** identifica las amenazas que se encuentran asociadas a la vulnerabilidad
g. **Amenazas:** identifica las amenazas asociadas a la vulnerabilidad identificada
h. **Controles asociados:** identifica los controles que mitigan/reducen la materialización o explotación de la vulnerabilidad
i. **Descripción del control:** identifica el nombre del control

3.3 Registro de riesgos en el sistema GRC-NOVASEC

A continuación, se muestran los pasos a seguir en el módulo de Riesgos de la herramienta GRC:

a. Ingresar al Módulo de Riesgos:

Ilustración 16. Menú riesgos

b. Dar clic en la opción “Gestión”:

Ilustración 17. Opción gestión, menú de riesgos

c. Dar clic en el botón + Agregar a continuación se despliega la siguiente pantalla donde se debe registrar el riesgo:

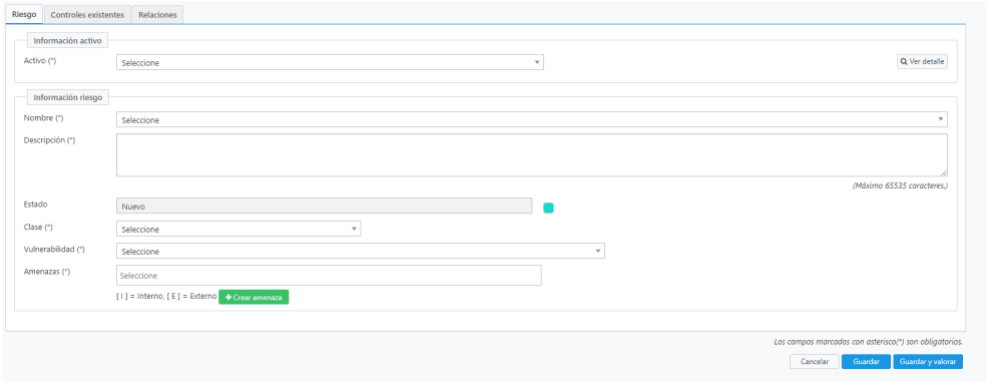


Ilustración 18. Ventana ingreso de riesgos

En esta sección se debe incluir la siguiente información:

- ☑ **Campo Activo:** seleccione de la lista desplegable el activo que desea realizar el análisis de riesgos de seguridad de la información teniendo en cuenta la depuración previa recomendada en el numeral 3.1 Generar el listado de los activos de información

- ☑ **Campo Nombre:** este campo permite incluir el tipo de riesgo al cual está expuesto el activo de información bien sea de Confidencialidad, Integridad y/o Disponibilidad (CID). Esta información fue identificada una vez se estaba realizando el levantamiento de activos de información. Para esto, identificar cuál o cuáles se calificaron como "ALTA".

  Nota: no se puede registrar 2 tipos de riesgo de manera simultánea, se debe realizar el registro de manera independiente

- ☑ **Campo Descripción:** este campo permite incluir el detalle del tipo de riesgo identificado como se detalla en el numeral 3.10.4. Estructura para describir el riesgo de la cartilla CT-IIt-0132 Gestión de riesgos de seguridad de la información:

- ☑ **Campo Estado:** este campo se autocompleta automáticamente.

- ☑ **Campo Clase:** en este campo se debe seleccionar la opción "Seguridad de la Información y protección de datos personales".

- ☑ **Campo Vulnerabilidad:** se debe seleccionar la vulnerabilidad de la lista desplegable relacionada con el activo de información. Se debe tener en cuenta:

  - Las principales vulnerabilidades se han identificado previamente y se debe considerar la tabla de vulnerabilidades que se encuentra en el Instrumento de consulta para la gestión de riesgos de seguridad de la información. En caso de identificar que existe una vulnerabilidad que no se encuentra registrada en el sistema, se debe contactar a la Oficina de Seguridad de la Información a través del buzón seguridaddigital@dian.gov.co para que se indique como realizar el registro de la vulnerabilidad en el sistema.

  - Las vulnerabilidades están identificadas dependiendo del tipo de activo: Información, Software, Hardware, Servicios, Infraestructura Física, Recurso Humano. Dependiendo de esta característica se debe realizar el análisis de la vulnerabilidad que puede afectar el activo de información que se está evaluando.

- ☑ **Campo Amenaza:** se debe seleccionar las amenazas que están relacionadas y que pueden sacar provecho de la vulnerabilidad.

  Nota: en caso de no identificar una amenaza para la vulnerabilidad identificada, se debe contactar a la Oficina de Seguridad de la Información a través del buzón seguridaddigital@dian.gov.co para incluir dicha amenaza y realizar el análisis correspondiente.

d. Por último, de debe dar clic en el botón “Guardar” para registrar la información en el sistema.

3.4 Calificar la probabilidad y el impacto

Para realizar la calificación de la probabilidad y el impacto, se debe tener en cuenta lo siguiente:

☑ Las fórmulas para de la probabilidad y el impacto fueron configuradas previamente y el sistema realizará el cálculo automático de acuerdo a la información ingresada.

A continuación, se muestran los pasos a seguir para el cálculo de la probabilidad y el impacto en la herramienta GRC.

a) Ingresar al Módulo de Riesgos:

Ilustración 19. Menú riesgos

b) Dar clic en la opción “Valoración”:

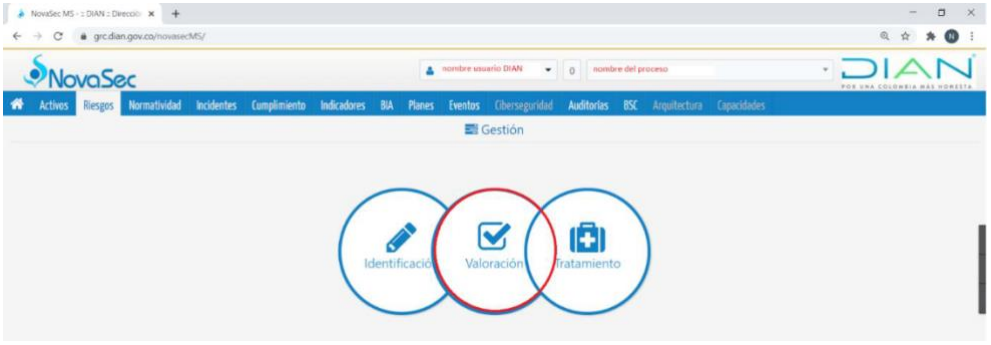


Ilustración 20. Opción valoración

c) En la pantalla aparece un listado con los riesgos identificados. Para hacer el proceso de valoración, dar clic en el botón “Acciones” y escoger la opción “Valoraciones”:

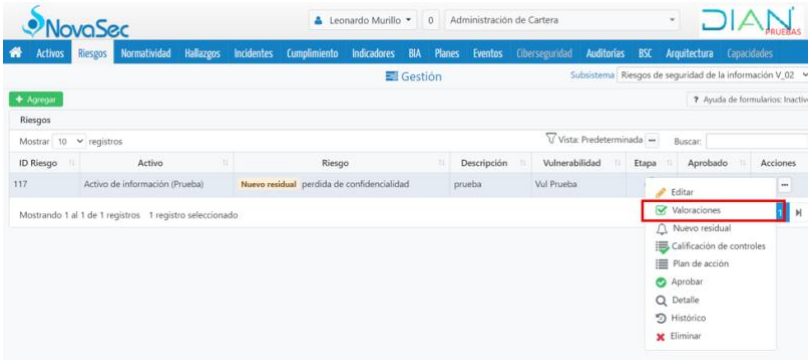


Ilustración 21. Opción para la valoración

d) El sistema muestra la siguiente pantalla con la información del riesgo:

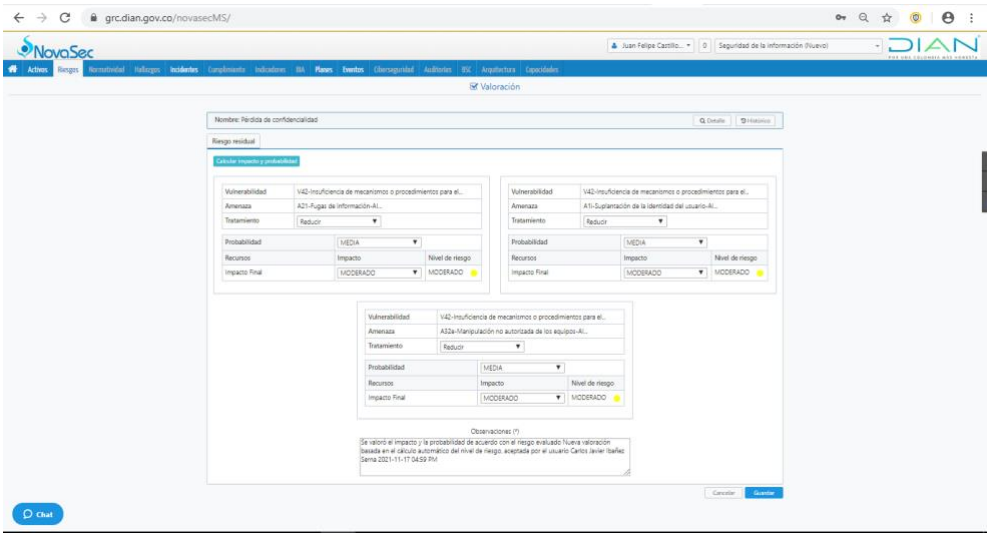


Ilustración 22. Ventana para la valoración de riesgos

Nota: en caso de dar clic en el botón “Detalle”, se muestra la siguiente información que fue capturada en la identificación del riesgo:

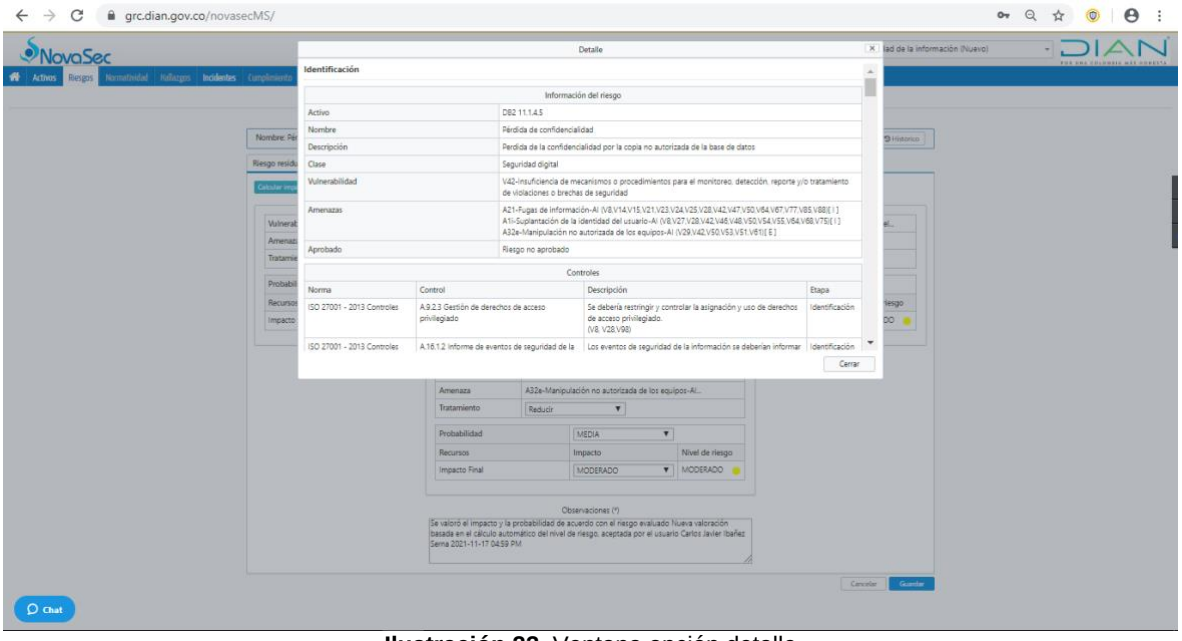


Ilustración 23. Ventana opción detalle

e. Seleccionar y Dar clic en el botón “Calcular impacto y probabilidad” para registrar los valores de estas variables

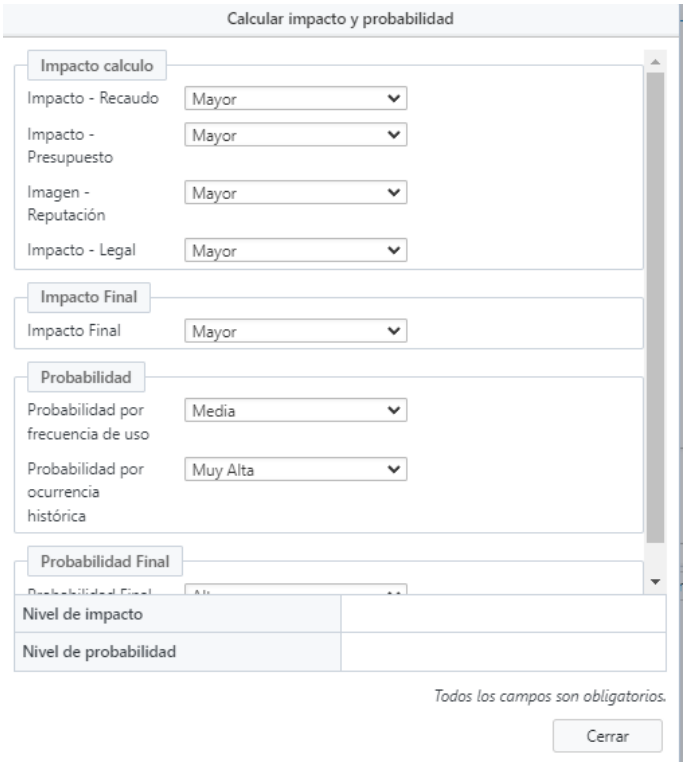


Ilustración 24. Ventana valoración probabilidad e impacto

Para evaluar el impacto se tienen en cuenta las siguientes dimensiones:

- ☑ Imagen - Reputación
- ☑ Económico - Recaudo
- ☑ Económico - Presupuesto
- ☑ Legal

El impacto final es el resultado del cálculo automático de los valores asignados en las dimensiones mencionadas.

Para evaluar la probabilidad se tienen en cuenta las siguientes dimensiones:

- ☑ Probabilidad por Frecuencia de Uso
- ☑ Probabilidad por Histórico de ocurrencia.

La probabilidad final es el resultado del cálculo de los valores asignados en las dimensiones mencionadas.

Nota: Para conocer el detalle de los valores tomados en los cálculos de cada variable de impacto y probabilidad, consultar el documento *CT-IIT-0132 Cartilla de Gestión de Riesgos de Seguridad de la Información*

Una vez realizado los cálculos automáticos de impacto y probabilidad se obtienen los resultados finales, como se muestran a continuación:

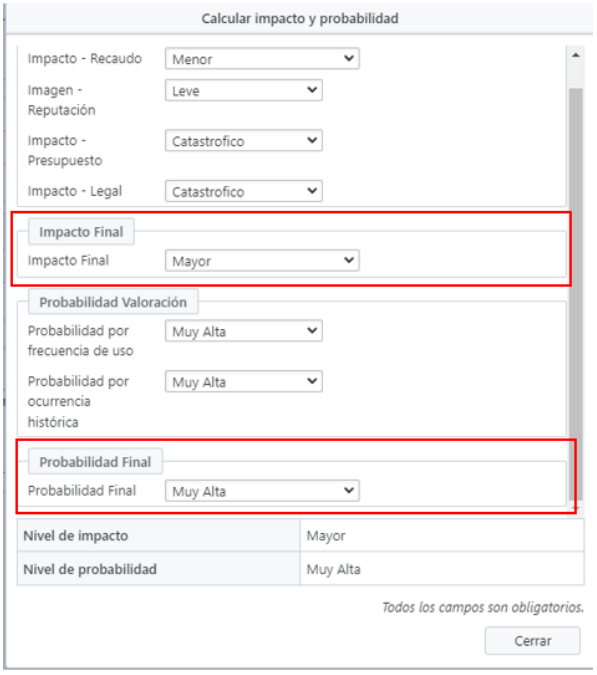


Ilustración 25. Venta calculo probabilidad e impacto final

La combinación de los cálculos de las variables impacto y probabilidad refleja como resultado el nivel de riesgo, información que es el insumo para definir el mapa de calor, de acuerdo con lo definido en la metodología para la gestión de riesgos de seguridad de la información que se puede encontrar en el documento *CT-IIT-0132 Cartilla de Gestión de Riesgos de Seguridad de la Información.*

f. Por último, dar clic en el botón “Cerrar”.

En la pantalla aparecen estos campos diligenciados: la probabilidad final, el impacto final y el nivel de riesgo:

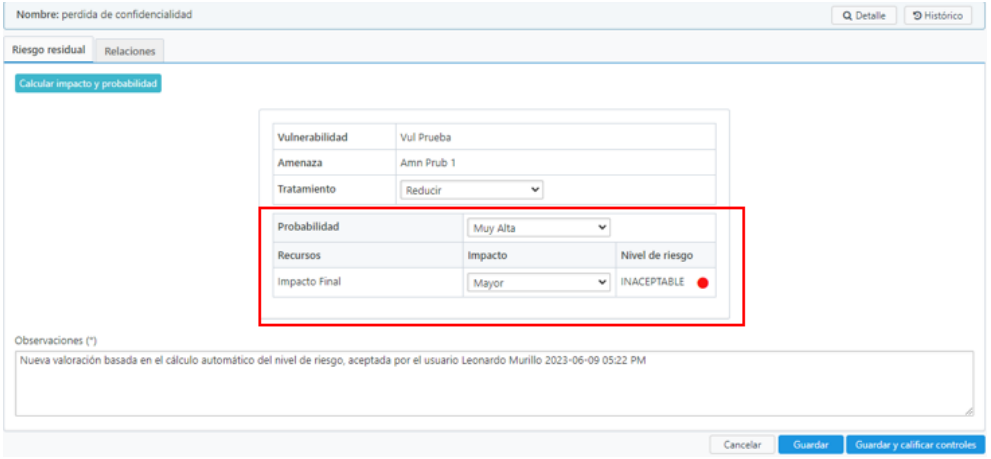


Ilustración 26. Ventana consolidación de valoración

3.5 Mapa del riesgo inherente de seguridad de la información

En la herramienta GRC el riesgo puro se denomina “Riesgo Inherente”.

Para obtener el Mapa, seguir los siguientes pasos:

a. Ingresar por la opción Riesgos – Reportes:

Ilustración 27. Menú riesgos, opción reportes

b. Escoger en el menú vertical la opción “Mapa de calor por proceso”:

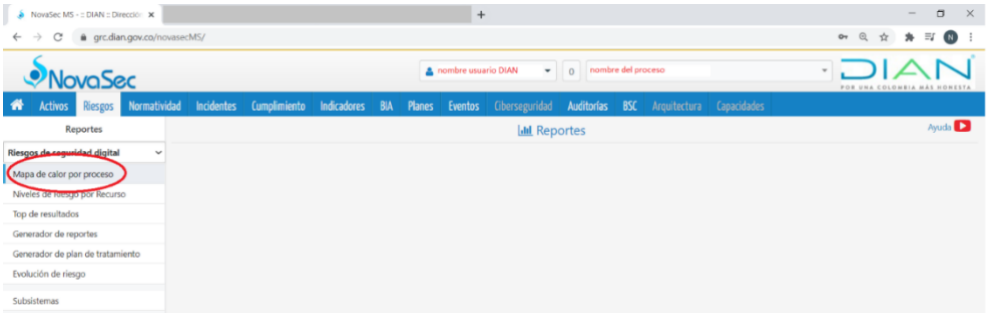


Ilustración 28. Generación mapa de calor de riesgos

La pantalla muestra el siguiente reporte:

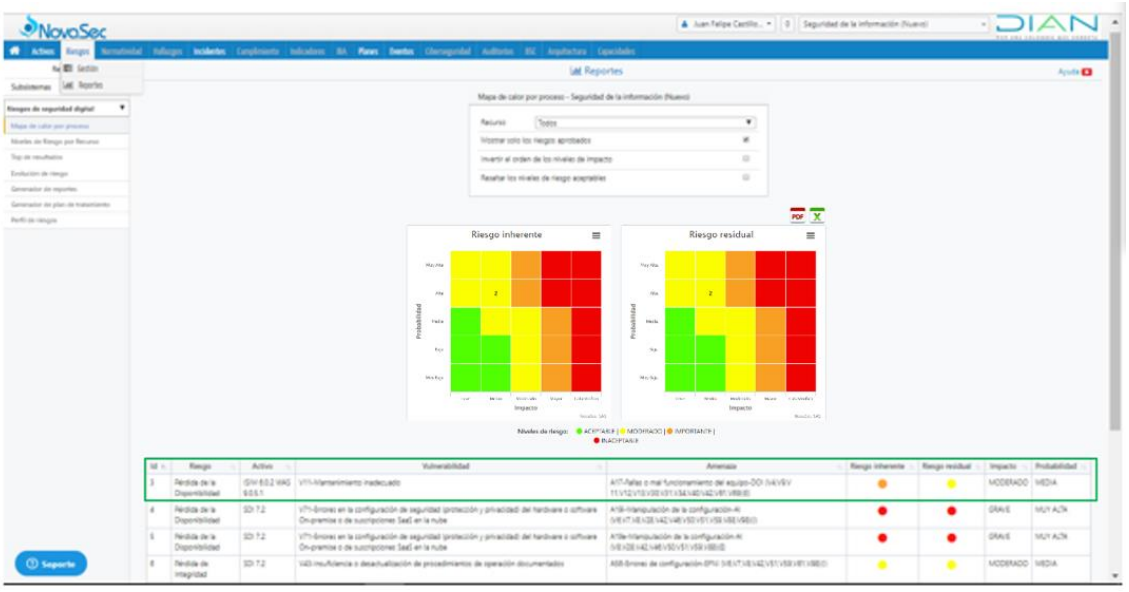


Ilustración 29. Reporte riesgo inherente y residual

Nota: Este reporte también se puede descargar en los formatos PDF y Excel, dando clic en los íconos

Ilustración 30. Opciones de generación de reportes

A manera de ejemplo, en este reporte se puede observar el riesgo inherente de uno de los riesgos en la parte izquierda identificado con el Id = 8 enmarcado con el cuadro rojo, hasta este momento se ubicó en la zona del mapa de calor amarilla, es decir con una calificación de “Moderado”.

En la misma gráfica, en la parte derecha se puede observar el mismo riesgo con la aplicación de

los controles, este se ubica en el mapa de calor en la zona de color “verde”, es decir con una calificación de “Aceptable”

En la parte inferior se muestra como ejemplo, la información de valoración del riesgo con Id = 3 donde se encuentra enmarcada toda la zona con el rectángulo verde.

3.6 Opciones de tratamiento de riesgo de seguridad de la información

a. En la pantalla del GRC, escoger el tipo de tratamiento del riesgo y escribir las observaciones pertinentes:

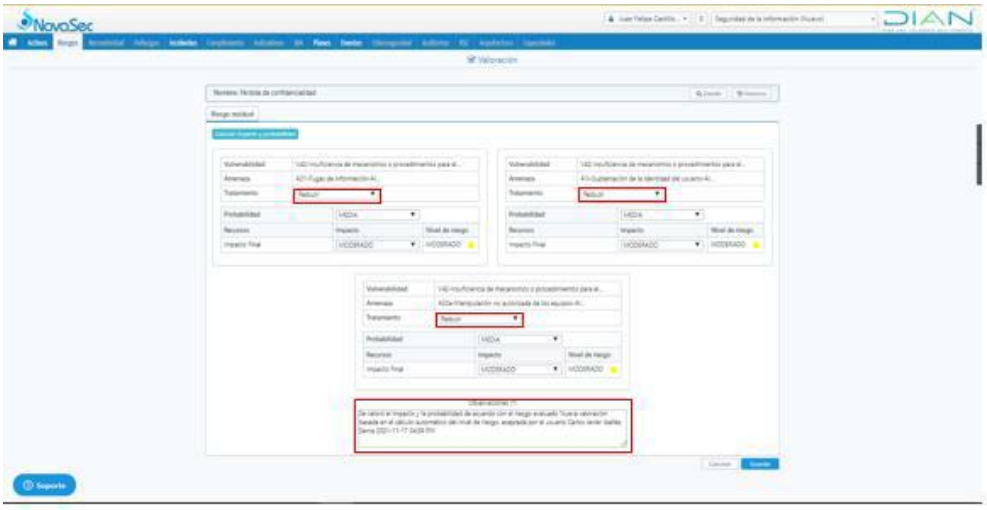


Ilustración 31. Ventana de opciones de tratamiento de riesgos

b. Seleccionar y dar clic en el botón “Guardar”.

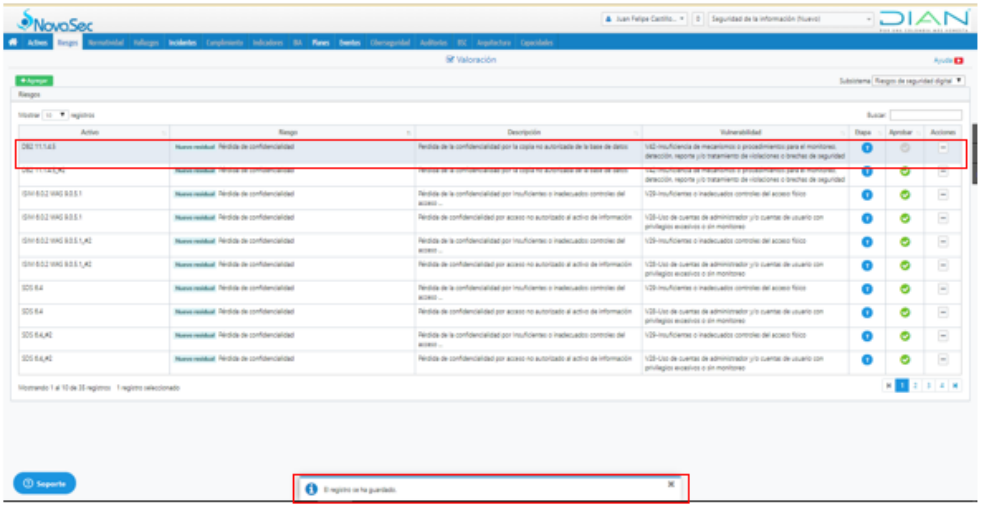


Ilustración 32. Ventana de consolidación de riesgos

3.7 Evaluación del control de seguridad de la información

3.7.1 Identificación de los controles

Como se describe en la sección *3.2.1 Instrumento de consulta para la gestión de riesgos de seguridad de la información* la entidad cuenta con controles previamente identificados. A continuación se relacionan algunos aspectos importantes para la gestión de los controles:

- ☑ La identificación de nuevos controles debe realizarse para cada riesgo a través de las entrevistas con los líderes de los procesos o servidores públicos expertos en sus actividades diarias.
- ☑ Los responsables de implementar, monitorear y hacer seguimiento a la efectividad de los controles son los líderes de los procesos con el apoyo de su equipo de trabajo.
- ☑ Para cada vulnerabilidad se identifica mínimo un control y un control puede ser utilizado para varias vulnerabilidades.
- ☑ Una política por sí sola no es un control. Los controles se despliegan a través de los procedimientos documentados.
- ☑ La actividad del control debe por si sola mitigar o tratar la causa del riesgo (vulnerabilidad) y ejecutarse como parte del día a día de las operaciones.
- ☑ Para la adecuada mitigación de los riesgos, no basta con que un control esté bien diseñado; el control debe ejecutarse por parte de los responsables tal como se diseñó.
- ☑ Un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

Para relacionar los controles con el riesgo identificado y medir el nivel de mitigación, se deben seguir las siguientes actividades:

a. Una vez se identifique el riesgo al cual se desea realizar la aplicación de controles, se debe deslizar el puntero del mouse hacia el borde derecho de la pantalla para ver la opción de “Calificación de controles”:

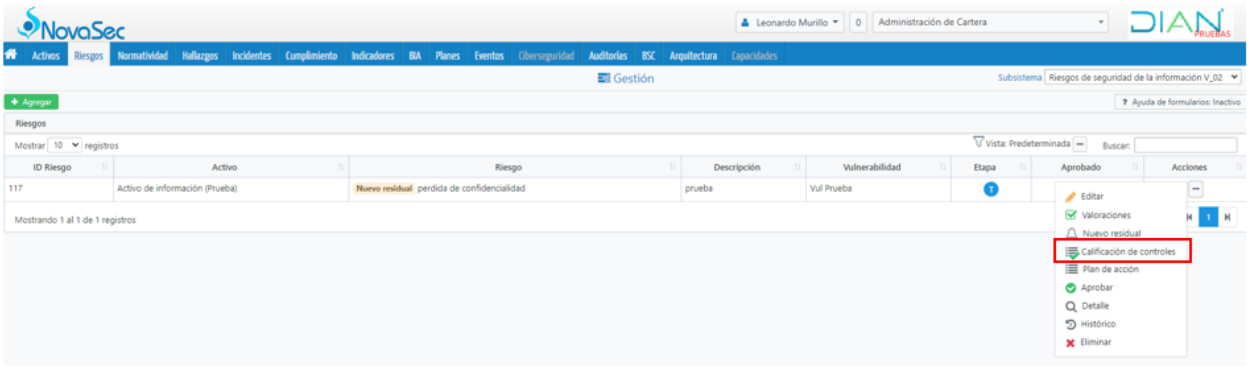


Ilustración 33. Opción de calificación de controles

b. Ubicados allí se debe seleccionar la opción “Agregar” y el sistema permitirá visualizar la siguiente vista:

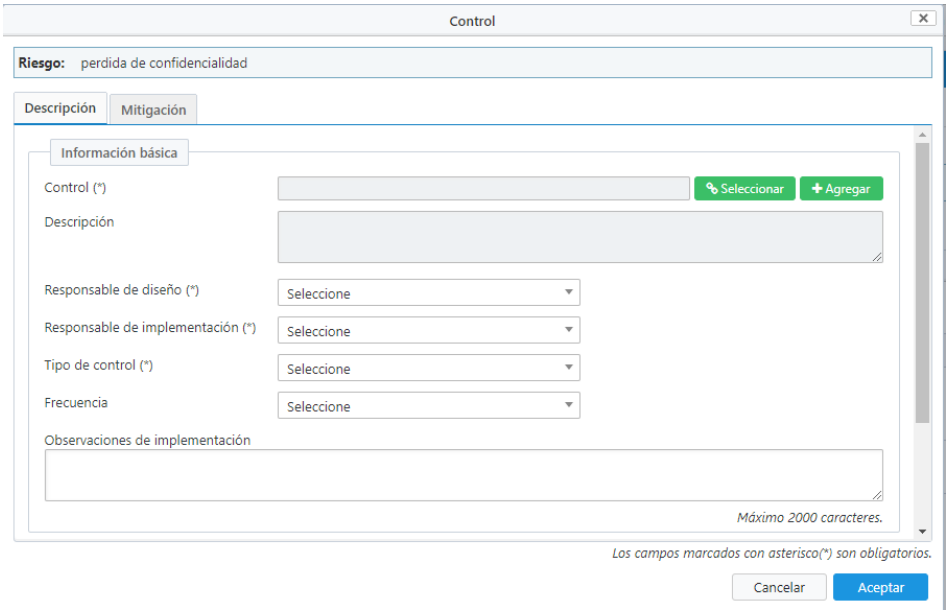


Ilustración 34. Ventana de gestión de controles

c. Ubicados en esta parte, se debe completar los campos con la siguiente información:

☑ **Campo control:** Se debe seleccionar el control previamente configurado e incluido en la herramienta. Se debe dar clic en la opción “Seleccionar” y el sistema permitirá visualizar la siguiente imagen:

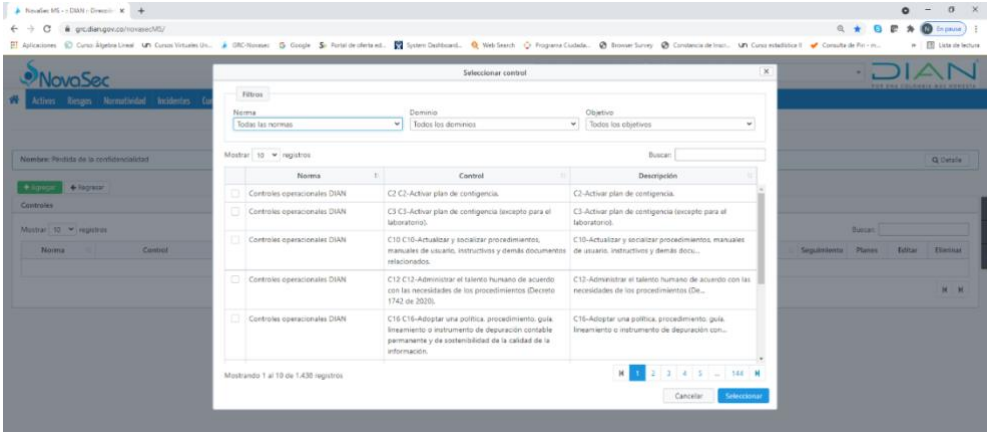


Ilustración 35. Ventana de selección de controles

Al seleccionar el control, el sistema quedará habilitado para continuar con la inclusión de la información.

Nota: se deben seleccionar controles que sean efectivos en la remediación del riesgo identificado, Los controles habilitados en el momento para la gestión de riesgos de seguridad de la información se pueden identificar en el *Instrumento de consulta para la gestión de riesgos de seguridad de la información* en la tabla de controles.

☑ **Campo descripción:** el sistema incluirá la información de manera automática de acuerdo con el control seleccionado en el “Campo control”

☑ **Responsable del diseño:** se debe seleccionar la dependencia que será la responsable del diseño del control

☑ **Responsable de la implementación:** se debe seleccionar la dependencia que será la responsable de la implementación

☑ **Tipo de control:** se debe seleccionar entre las opciones Preventivo / Detectivo (en dado caso que el control mitigue la variable de probabilidad) o Correctivo (en dado caso que en el control mitigue la variable de impacto).

☑ **Frecuencia:** se debe seleccionar la frecuencia de aplicación del control entre diario, semanal, mensual, bimestral, trimestral, semestral, anual, otro, por demanda y permanente.

☑ **Observaciones de implementación:** espacio en donde se deben incluir las características de la implementación del control o información importante que el enlace de seguridad desee aportar.

- ☑ **Información Adicional del control:** se deben seleccionar las opciones “Ejemplo” en los dos campos de esta sección

d. Una vez diligenciada la información del formulario anterior, el usuario se debe dirigir a la opción “Mitigación”

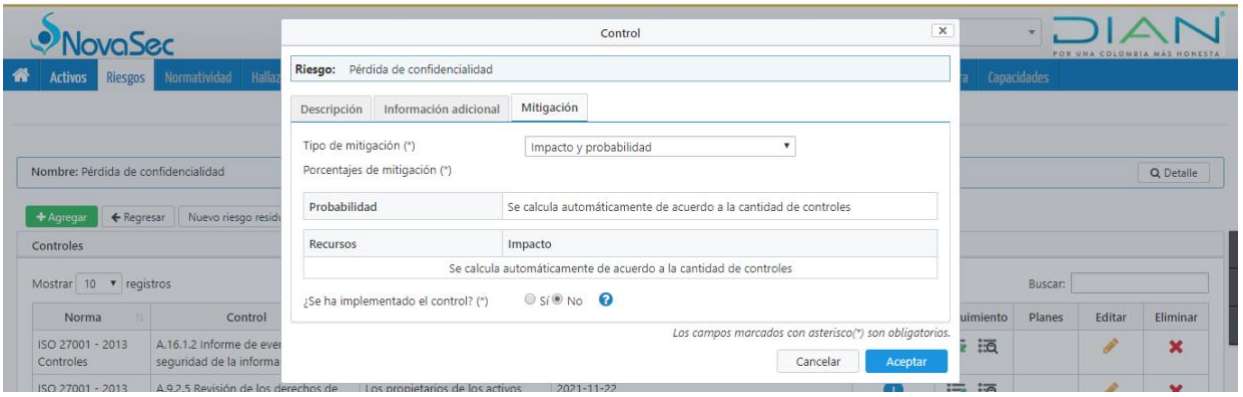


Ilustración 36. Opción de mitigación, ventana de selección de controles

Ubicados en esta parte el usuario debe seleccionar los siguientes campos:

- ☑ **Tipo de mitigación:** se debe seleccionar si el control mitigará la probabilidad (Si el control es detectivo o preventivo) o si mitigará el impacto (si el control es correctivo).
- ☑ **Porcentajes de mitigación**: el sistema realizará el cálculo automático de este campo.
- ☑ **Campo “¿Se ha implementado el control?”:** se debe seleccionar si el control se encuentra o no implementado en la dependencia.

3.7.1.1 Evaluación de controles

Los controles que no sean categorizados como “trasversales” deben ser calificados de manera *independiente* una vez sean seleccionados, para realizar este paso se debe realizar lo siguiente:

a. Ubicarse en la sección de “tratamiento” y ubicar el control que se requiere calificar, luego de ello seleccionar los tres puntos en la parte derecha de la pantalla en la opción acciones para que el sistema le permita seleccionar al usuario la opción “Agregar seguimiento”

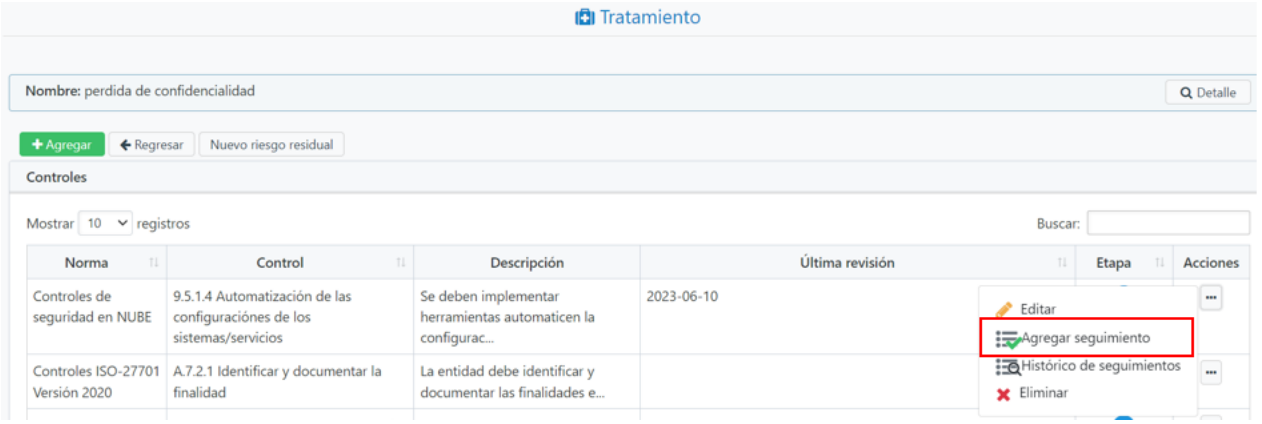
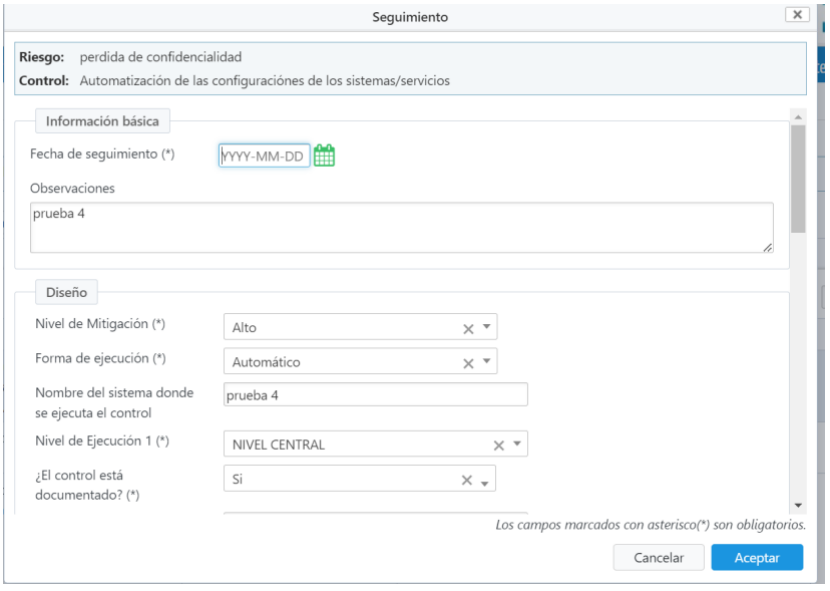


Ilustración 37. Selección para realizar el seguimiento

b. Ubicados en la pantalla emergente se debe ingresar la siguiente información:



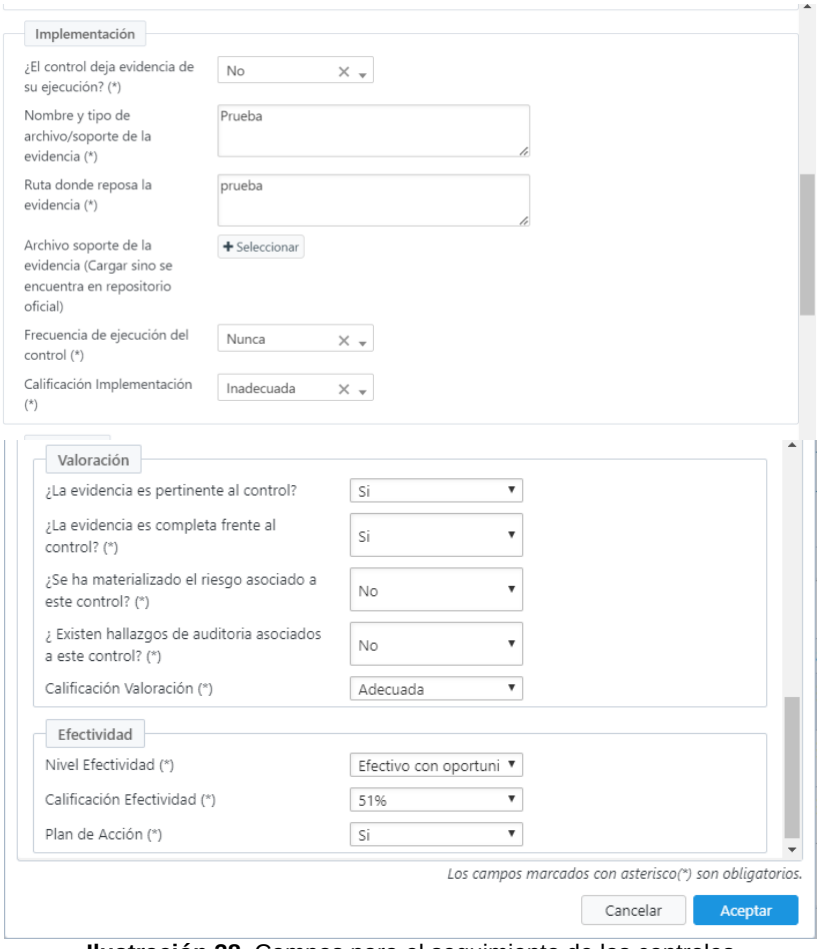


Ilustración 38. Campos para el seguimiento de los controles

A continuación, se observan con más detalle los valores diligenciados en el ejemplo.

Los campos señalados con las flechas los calcula automáticamente la herramienta GRC y corresponden a las calificaciones individuales del control respecto a su Diseño, Implementación y Efectividad, de acuerdo con lo establecido en la *Cartilla para la gestión de riesgos de seguridad de la información* en la sección *3.11.2. Atributos para la evaluación individual de controles*

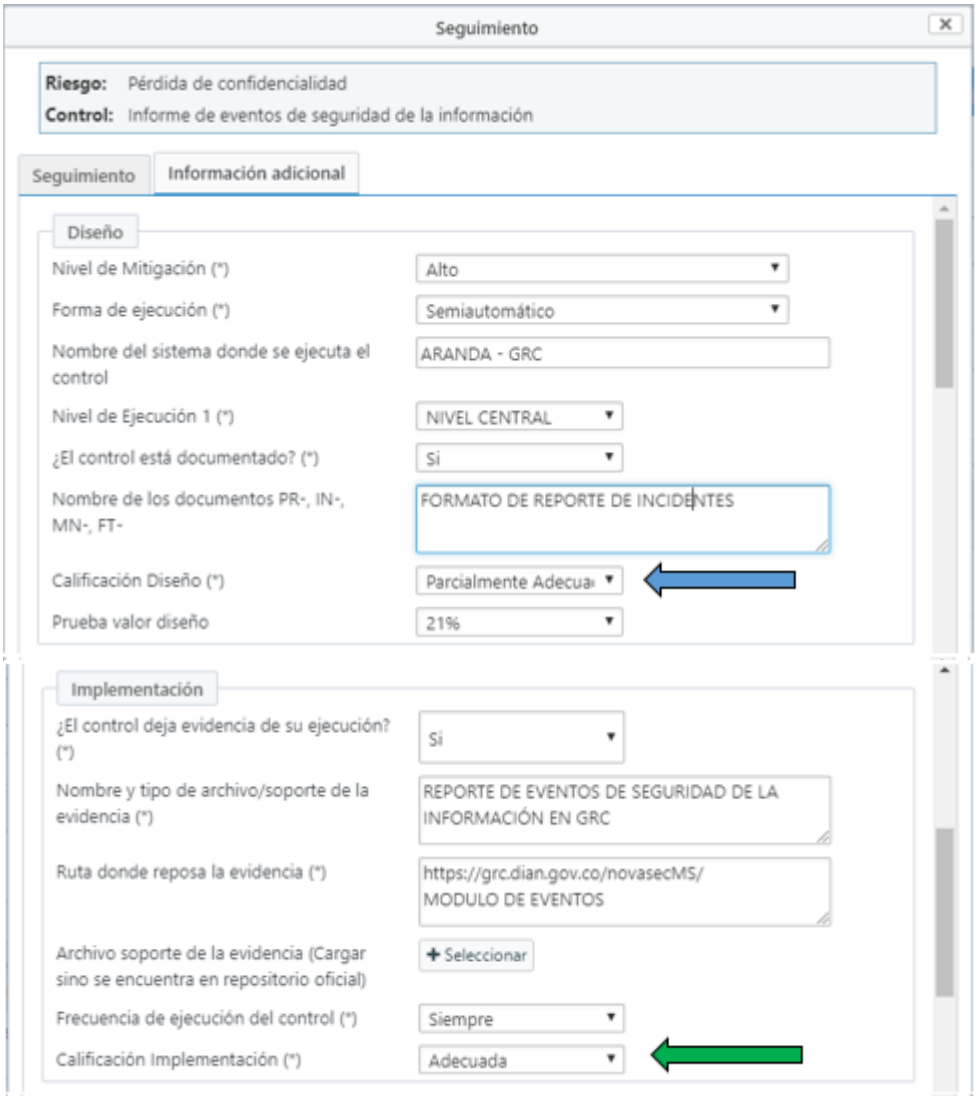

Seguimiento
Riesgo: Pérdida de confidencialidad
Control: Informe de eventos de seguridad de la información
Seguimiento
Información adicional
Diseño
Nivel de Mitigación (*)
Alto
Forma de ejecución (*)
Semiautomático
Nombre del sistema donde se ejecuta el control
ARANDA - GRC
Nivel de Ejecución 1 (*)
NIVEL CENTRAL
¿El control está documentado? (*)
Si
Nombre de los documentos PR-, IN-, MN-, FT-
FORMATO DE REPORTE DE INCIDENTES
Calificación Diseño (*)
Parcialmente Adecua
Prueba valor diseño
21%
Implementación
¿El control deja evidencia de su ejecución? (*)
Si
Nombre y tipo de archivo/soporte de la evidencia (*)
REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN EN GRC
Ruta donde reposa la evidencia (*)
https://grc.dian.gov.co/novasecMS/ MODULO DE EVENTOS
Archivo soporte de la evidencia (Cargar sino se encuentra en repositorio oficial)
+ Seleccionar
Frecuencia de ejecución del control (*)
Siempre
Calificación Implementación (*)
Adecuada

Ilustración 39. Campos de cálculo automático

3.7.1.2 Selección de controles transversales

La entidad ha determinado incluir algunos controles basados en buenas prácticas y normas internacionales con el fin de apoyar el cumplimiento de la gestión de riesgos de seguridad de la información, algunos de estos controles son de aplicación individual y la responsabilidad es de cada dependencia. Otros si bien están bajo la responsabilidad de una dependencia en específico, su aplicación es transversal, esto son denominados como “Controles Transversales”

Para aplicar un control transversal se deben realizar las actividades incluidas en el numeral *3.7.1 Identificación de los controles* en las secciones a) y b) para luego realizar el siguiente cambio:

a. Ubicados en la ventana de diligenciamiento del control se debe seleccionar la opción de “utilizar como control transversal” esta opción permitirá al usuario traer automáticamente la calificación que se ha dado previamente por parte del responsable del control, y automáticamente aplicará los calculo para reducir los resultados en cuanto a la probabilidad o impacto dependiendo el caso

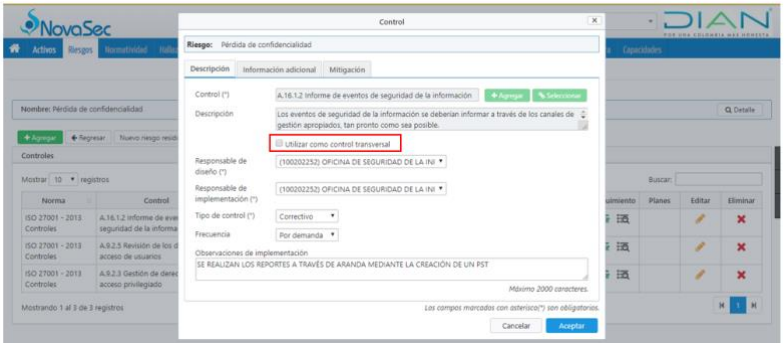


Ilustración 40. Selección de controles transversales

3.7.1.3 Evaluación de controles transversales

La evaluación de los controles transversales es una actividad que debe ser realizada por el responsable de la implementación del control con el acompañamiento de la Oficina de Seguridad de la Información. Para realizar el ejercicio de evaluación, en la herramienta GRC seguir los siguientes pasos:

a. Ingresar por Riesgos – Administración:

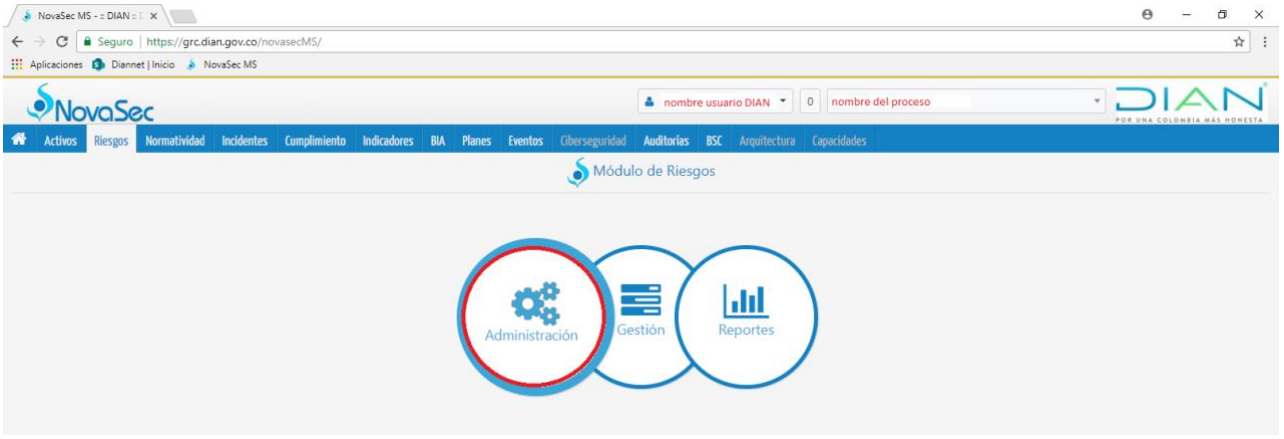


Ilustración 41. Menú riesgos, opción administración

b. Dar clic en la opción “Controles transversales”:

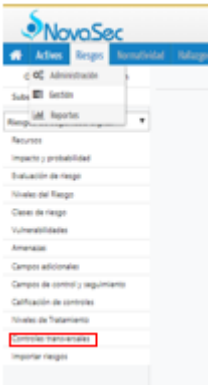


Ilustración 42. Menú selección seguimiento controles transversales

c. Se muestra un listado con todos los controles previamente incluidos tomados con base en el *instrumento de consulta para la gestión de riesgos de seguridad de la información que se encuentra en DIANNET,* como se muestra a continuación:

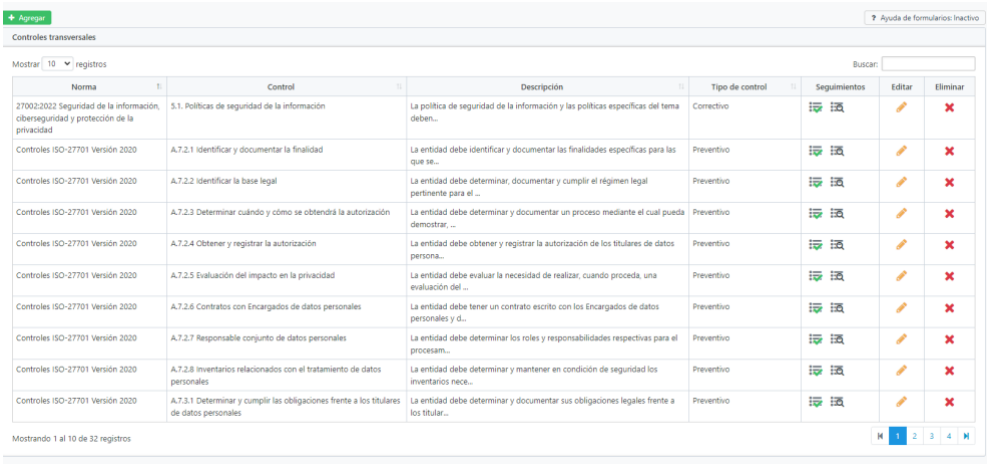


Ilustración 43. Listado de controles transversales

d. Para verificar y/o modificar la información básica del control dar clic en el botón “Editar”:

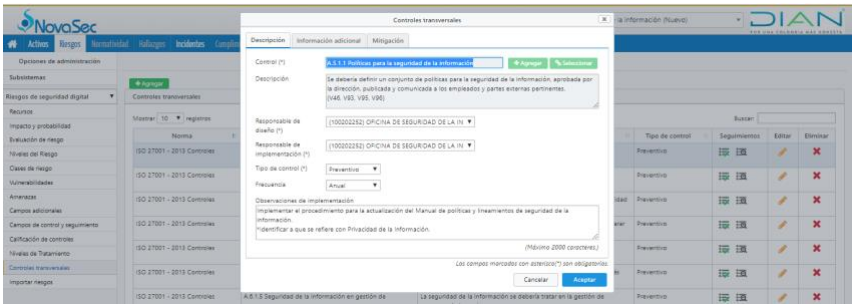


Ilustración 44. Ventana de edición del control

En la sección de Información adicional se debe diligenciar con la opción “ejemplo”:

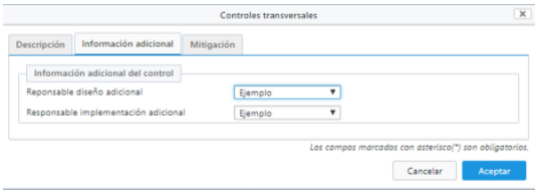


Ilustración 45. Ventana de selección de control, opción de información adicional

En la pestaña “mitigación” se debe seleccionar si el control se encuentra mitigando la variable de probabilidad (cuando el control es detectivo o preventivo) o el impacto (cuando el control es correctivo):

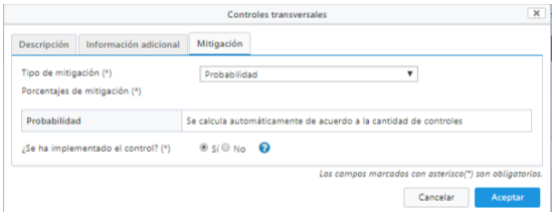


Ilustración 46. Ventana de selección de control, opción de mitigación

Por último, se debe seleccionar la opción “si” en el campo “*Se ha implementado el control?*” y dar clic en el botón aceptar.

Nota: para realizar la evaluación o seguimiento del estado del control una vez se haya incluido, se deben seguir las actividades descritas en el numeral *3.7.1.1 Evaluación de controles* de este documento y siguiendo las definiciones que se encuentra en el documento *CT-IIT-0132 Gestión de riesgos de seguridad de la información*.

1.1.1. Evaluación efectividad conjunta de controles

La calificación de controles se realiza de manera conjunta y automática en GRC – NOVASEC. Cada vez que se realiza la inclusión de un nuevo control o se realiza la edición del riesgo que se está evaluando, se activa la pestaña “Nuevo riesgo residual” en la pantalla de Riesgos-Gestión-Tratamiento.

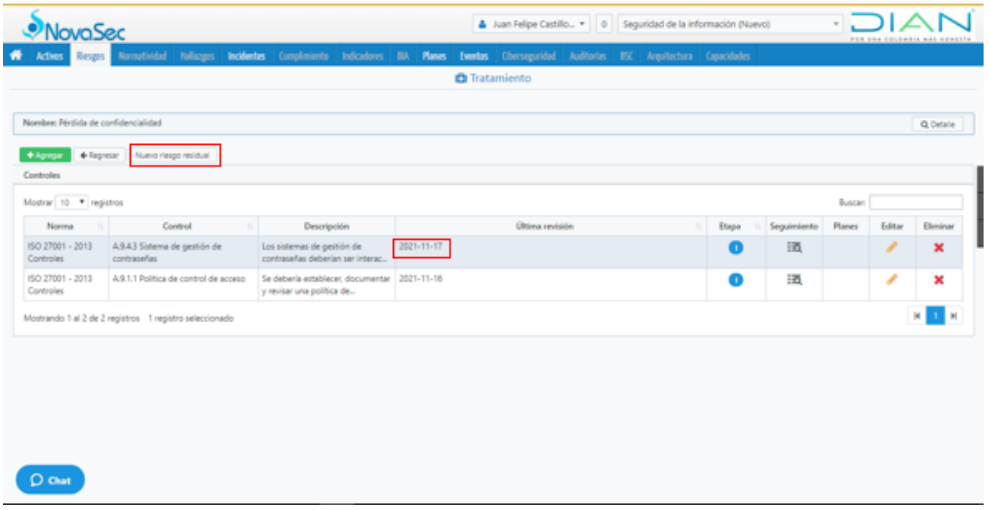


Ilustración 47. Ventana de selección “nuevo riesgo residual”

En el ejemplo, se tiene en cuenta únicamente el primer control, cabe destacar que los controles que tienen seguimiento guardado son los que tienen diligenciada la fecha en el campo “Última Revisión”, al dar clic en la pestaña “Nuevo riesgo residual”, aparece la siguiente ventana:

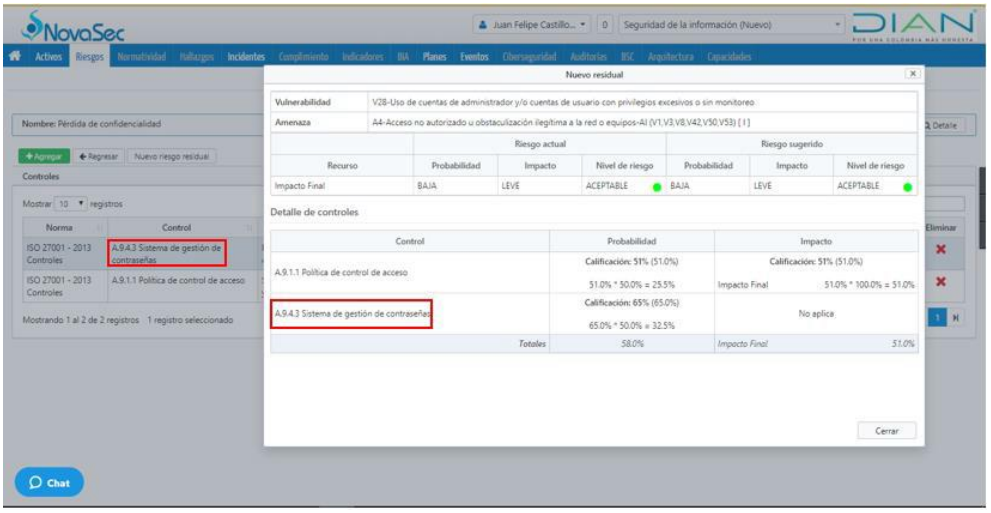


Ilustración 48. Ventana de visualización resultados riesgo residual

Como se observa, para el cálculo de la evaluación conjunta de controles, solamente se tuvo en cuenta el control de la ISO 27001 A.9.4.3, aunque el otro control también tiene seguimiento.
En el siguiente ejemplo, se realizará el seguimiento a los tres (3) controles identificados para que se pueda observar la evaluación conjunta de controles:

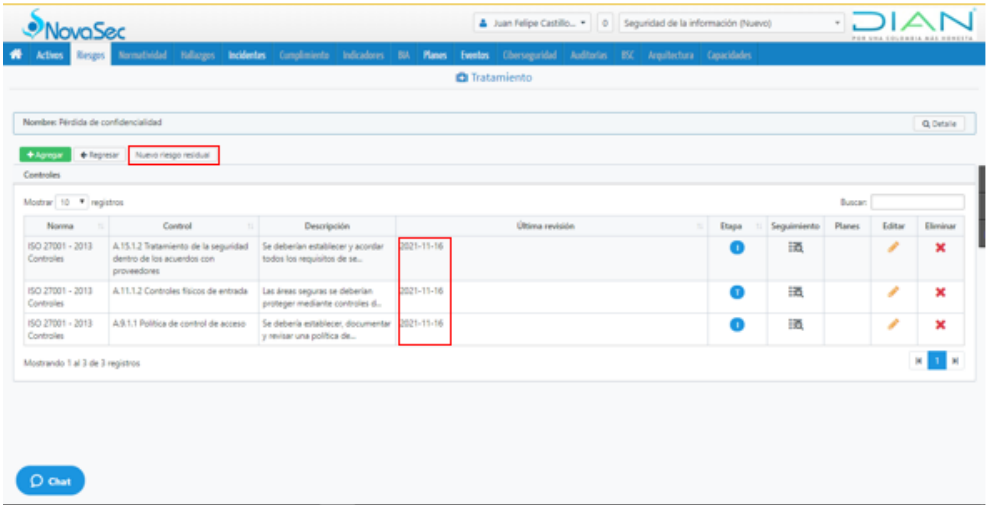


Ilustración 49. Ventana de valoración conjunta de controles

Al dar clic en el botón “Nuevo riesgo residual”, se observa que la evaluación conjunta de controles tuvo en cuenta los tres (3) controles y que a cada uno le da su respectiva calificación tanto en la probabilidad como en el impacto:

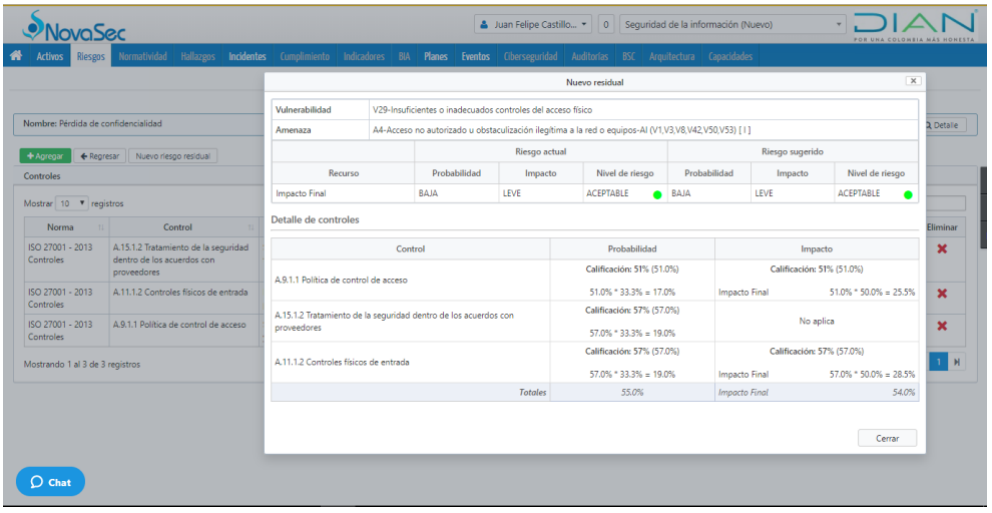


Ilustración 50. Ventana de transición del riesgo

Cada vez que se incluyan nuevos seguimientos al control, por ejemplo, cuando se tenga una mejora o decrecimiento en los controles calificados de manera individual se calculará un nuevo riesgo residual.

3.8 Generación del mapa de riesgo residual

Con base en los resultados obtenidos de la calificación conjunta de los controles de cada riesgo, se obtiene el mapa de riesgos residual a través del cual se visualizan los riesgos en un plano

cuyas coordenadas representan su probabilidad e impacto:

Probabilidad							
	100%	Muy Alta	Moderado	Moderado	Importante	Inaceptable	Inaceptable
	80%	Alta	Moderado	Moderado	Importante	Inaceptable	Inaceptable
	60%	Media	Aceptable	Moderado	Moderado	Importante	Inaceptable
	40%	Baja	Aceptable	Aceptable	Moderado	Importante	Inaceptable
	20%	Muy baja	Aceptable	Aceptable	Moderado	Importante	Inaceptable
			Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
					Impacto		

Ilustración 51. Mapa de calor

Para obtener los mapas de riesgo inherente y riesgo residual, realizar los siguientes pasos:

a. Dar clic en el botón “Reportes” del menú de Riesgos:

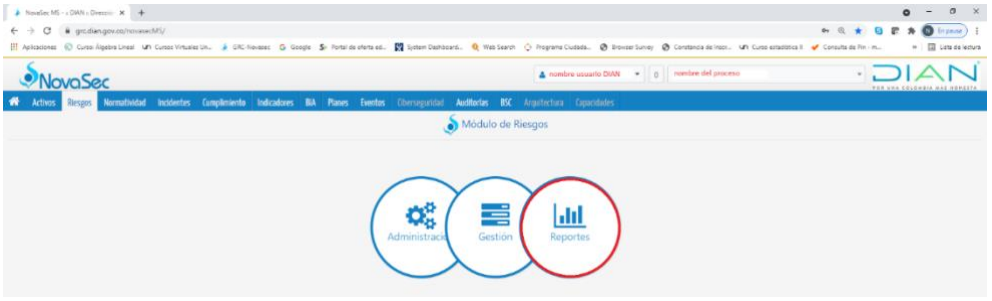


Ilustración 52. Menú de riesgos, opción reportes

b. Escoger en el menú vertical la opción “Mapa de calor por proceso”:

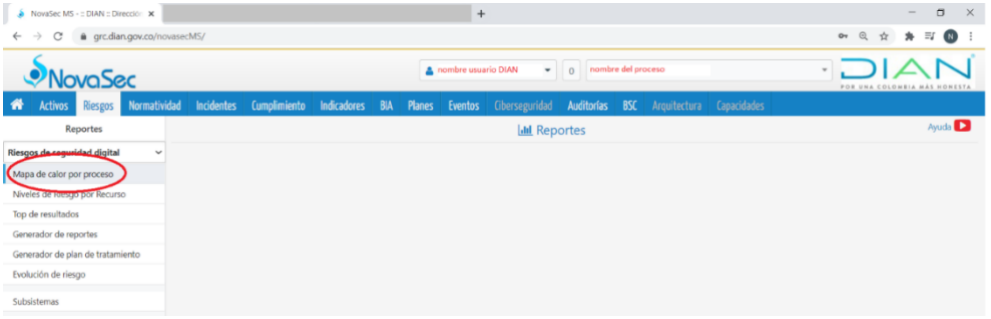


Ilustración 53. Generación de mapa de calor por proceso

c. Se muestra la siguiente pantalla con el mapa de calor del riesgo Inherente a la izquierda, y el mapa de calor del riesgo residual a la derecha:

Ilustración 54. Ventana de selección de control, opción de información adicional

En la *Ilustración 50. Ventana de selección de control*, opción de información adicional, en la parte izquierda se puede observar el riesgo inherente identificado con el Id = 8 enmarcado con el cuadro rojo, una vez evaluadas las variables de probabilidad e impacto. Este se ubica en la zona del mapa de calor color “amarilla”, lo que significa que su calificación es “Moderado”.

En esta misma gráfica*, se observa*, en la parte derecha se puede identificar el mapa de riesgo residual, para el riesgo con Id = 8 enmarcado con el cuadro rojo, una vez fueron relacionados los controles para mitigar su probabilidad e impacto. Este aparece en la zona de mapa de calor color “verde”, lo que significa que su calificación es “Aceptable”

Analizando lo anterior, al evaluar el conjunto de controles para este riesgo, se determinó que estos reducen el impacto por lo que el riesgo se desplazó a otra zona del mapa. En la gráfica *Ilustración 50. Ventana de selección de control*, en la parte inferior, se muestra como ejemplo la información de valoración del riesgo con Id = 3 donde se encuentra enmarcada toda la zona con el rectángulo verde.

3.9 Planes de tratamiento de riesgo de seguridad de la información

3.9.1 Creación de los planes de tratamiento

La creación del plan de tratamiento del riesgo de seguridad de la información debe ser realizado por el enlace de seguridad quien es el rol responsable y autorizado para ejecutar este tipo de actividades.

Se debe realizar las siguientes actividades en la herramienta GRC NOVASEC:

a. Ingresar a través del menú “Riesgos” a través de la opción “Gestión”:

Ilustración 55. Menú de riesgos, opción de gestión

b. Se debe buscar el riesgo al cual se debe establecer el plan de tratamiento de riesgo y seleccionar la opción “acciones”:

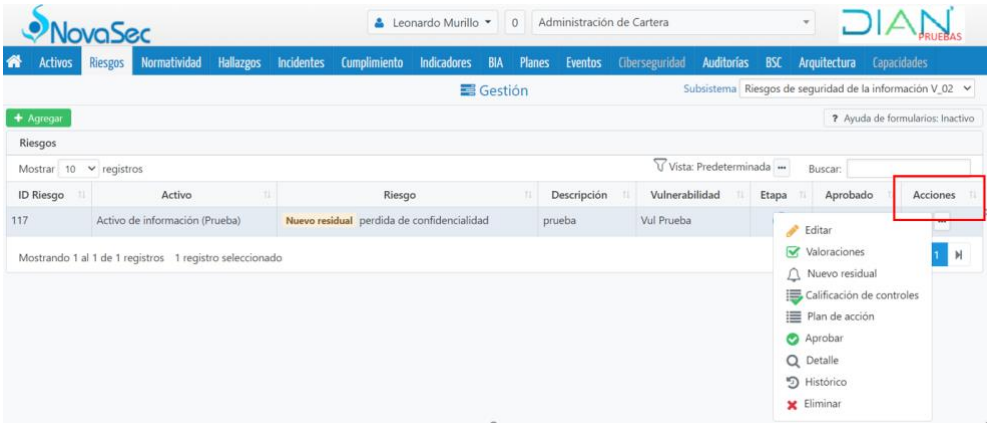


Ilustración 56. Menú acciones, opción plan de acción

Ubicados en la opción “Acciones” el usuario debe seleccionar la opción “Plan de acción” a lo cual el sistema le permitirá visualizar la siguiente ventana:

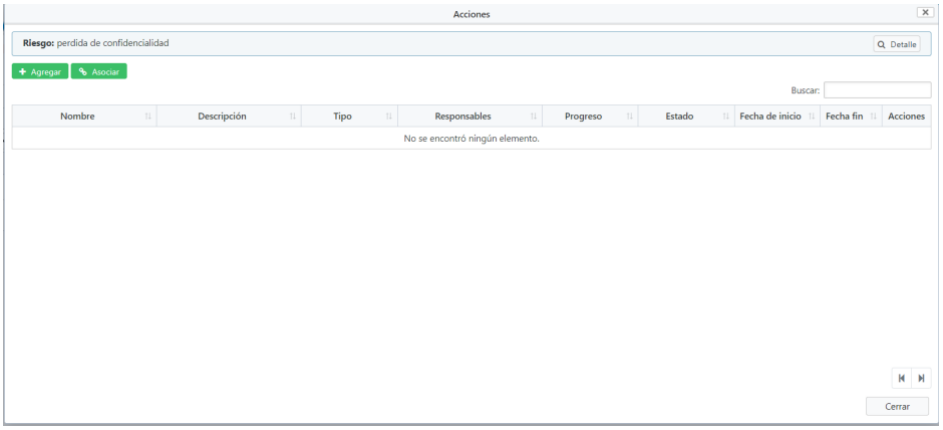


Ilustración 57. Ventana de inclusión de planes de tratamiento

c. En esta ventana el usuario debe seleccionar la opción “Agregar” y el sistema le permitirá visualizar la siguiente ventana:

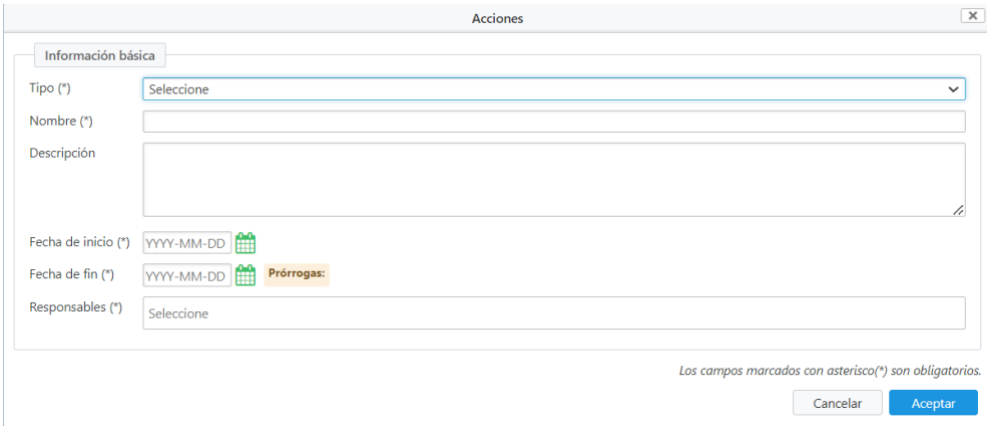


Ilustración 58. Ventana de ingreso de información de plan de tratamiento

d. En esta ventana, el usuario debe diligenciar la siguiente información:

- ☑ **Campo Tipo:** se debe seleccionar si el plan de tratamiento corresponde a una acción preventiva, correctiva o de mejora dependiendo la calificación final del control.
- ☑ **Campo Nombre:** se debe incluir el nombre del plan de acción
- ☑ **Campo Descripción:** se debe incluir una pequeña descripción del objetivo del control y las actividades detalladas que deben cumplirse para la finalización del plan de tratamiento
- ☑ **Campo Fecha de Inicio:** fecha en la cual se establece el plan de tratamiento
- ☑ **Campo Fecha Fin:** fecha propuesta para la finalización del plan de tratamiento
- ☑ **Campo Responsable:** incluir el nombre de la persona responsable de la ejecución

del plan de tratamiento

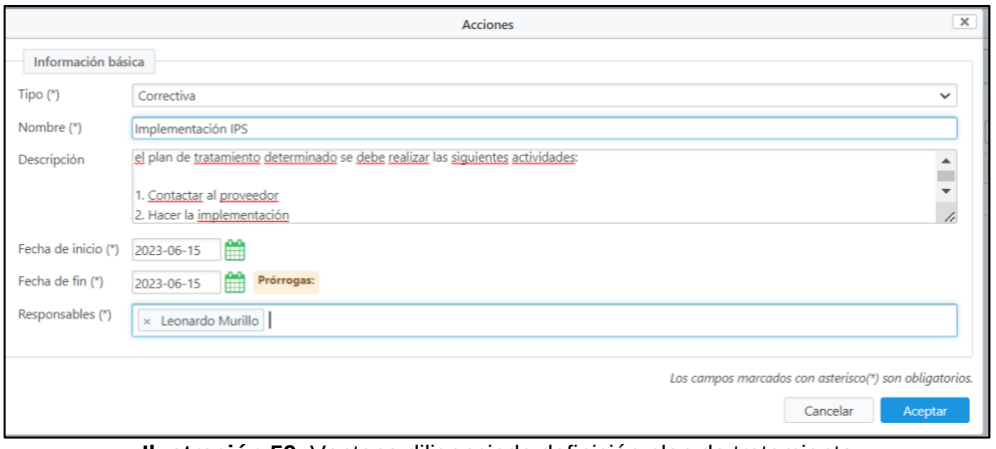


Ilustración 59. Ventana diligenciada definición plan de tratamiento

Luego de incluir la información se debe dar clic en el botón de “Aceptar”

e. El sistema creará el plan de tratamiento visualizando la siguiente información:

Ilustración 60. Ventana de inclusión de planes de tratamiento

Ubicado allí el usuario podrá actualizar el estado del plan de tratamiento y deberá realizar el registro correspondiente. Para visualizar la información actual del plan de tratamiento se debe seleccionar la opción “Acciones” y dar clic en el submenú “Detalle” el sistema le permitirá al usuario visualizar la siguiente ventana:

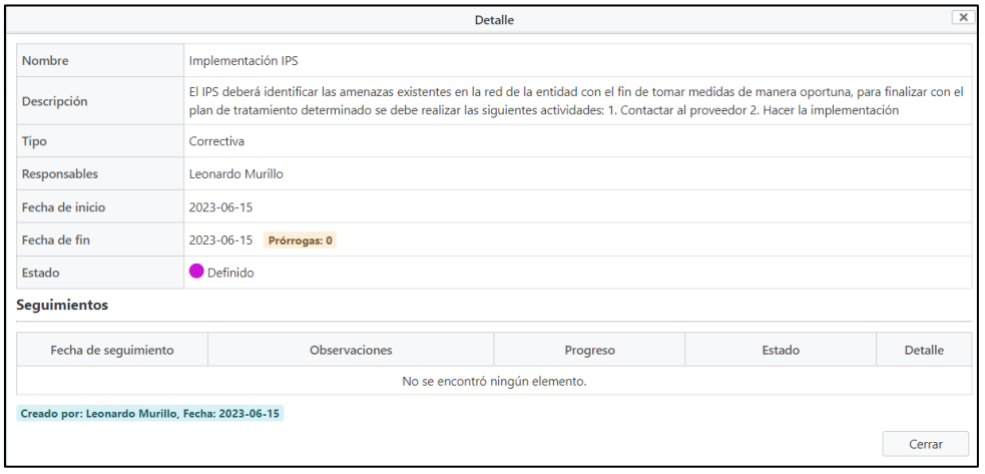


Ilustración 61. Ventana de detalle plan de tratamiento

3.9.2 Seguimiento planes de tratamiento de riesgos de seguridad de la información

Para realizar los seguimientos a los planes de tratamiento, el usuario debe seguir los siguientes pasos, ya descritos a lo largo del presente documento:

a. Ingresar por el menú de “Riesgos”
b. Seleccionar el submenú “Gestión”
c. Buscar el riesgo al cual le va a realizar el seguimiento de los planes de tratamiento
d. Ubicado en el riesgo, se debe selección los 3 (tres puntos) en la opción de acciones y seleccionar la opción “Plan de acción”, ubicados en el sistema le permitirá al usuario visualizar la siguiente pantalla:

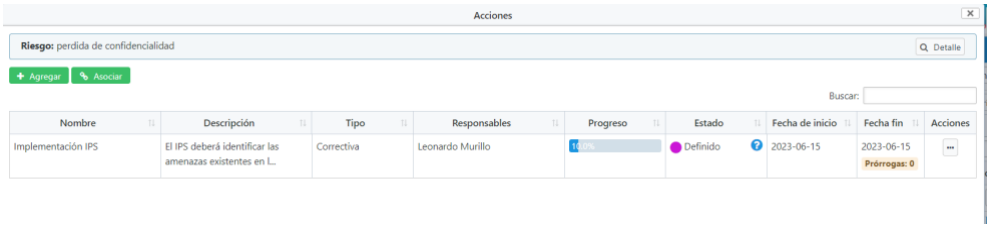


Ilustración 62. Ventana diligenciada definición plan de tratamiento

e. Ubicado en esta ventana el usuario debe seleccionar los 3 (tres puntos) en la opción de acciones y seleccionar la opción “Seguimiento”, ubicados allí el sistema le permitirá al usuario visualizar la siguiente pantalla:

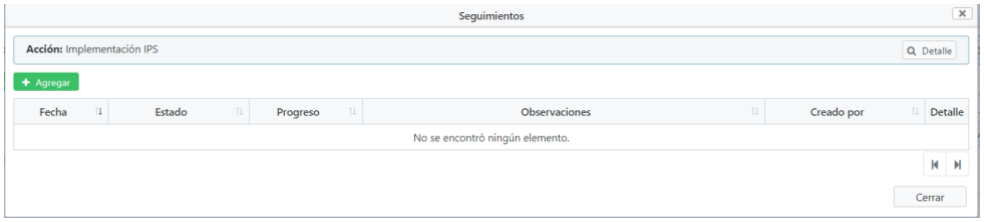


Ilustración 63. Ventana de inclusión de planes de tratamiento

f. Ubicados en esta ventana el usuario debe seleccionar la opción “Agregar” una vez realizado esto, el sistema le permitirá visualizar la siguiente ventana:

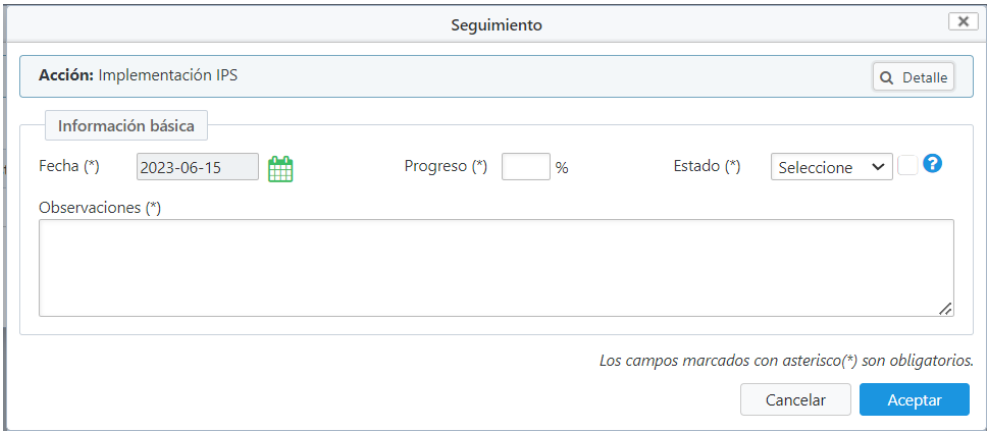


Ilustración 64. Ventana de inclusión de seguimiento planes de tratamiento

En esta ventana el usuario debe incluir la información de seguimiento diligenciando los siguientes campos:

- **Campo Fecha:** se debe ingresar la fecha en la cual se está realizando el seguimiento
- **Campo Progreso:** este campo será diligenciado de manera automática por el sistema
- **Campo Estado:** el campo estado se habilitará automáticamente por el sistema partiendo de un estado anterior de acuerdo a la configuración realizada en el sistema:

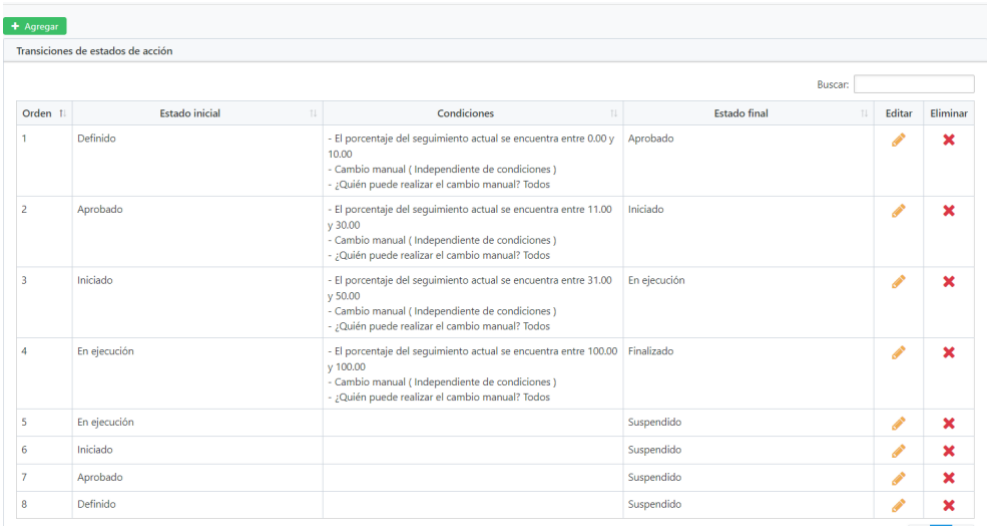


Ilustración 65. Ventana de transición de estado planes de tratamiento

El cambio de un estado a otro dependerá del avance del plan de acción de acuerdo a la siguiente información:

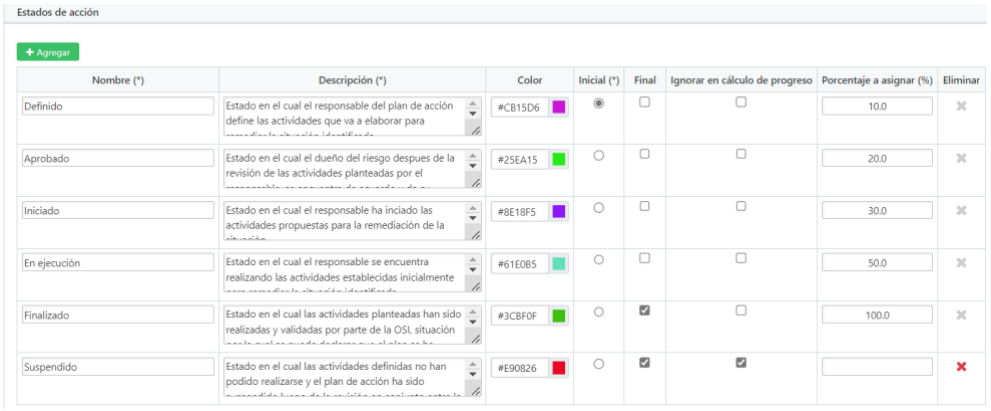


Ilustración 66. Ventana de estados de los planes de tratamiento

Solo se podrá seleccionar en cada seguimiento el valor identificado como el siguiente y no se podrá saltar los diferentes estados, Ejemplo: No se puede saltar el estado “Definido” al estado “Finalizado” sin pasar por los estados “Aprobado”, “Iniciado”, “En Ejecución” respectivamente.

El primer estado en el que nace el plan de tratamiento es el estado “Definido” que se crea una vez se establecen las condiciones y objetivos del plan de tratamiento, seguido del estado “Aprobado” que es cuando el responsable aprueba lo definido, seguido del estado “Iniciado” que es cuando se desarrollan las actividades iniciales propuestas, seguido del estado “En ejecución” que es cuando se tiene un adelanto significativo pero aún no se puede dar por terminado y por último el estado “Finalizado” cuando se identifique que se han cumplido con todas las actividades propuestas.

Nota: en caso de ser necesario el usuario responsable de la implementación del plan de tratamiento puede declarar como suspendido el plan de tratamiento de riesgos y deberá incluir la justificación en el sistema, para que sea revisado por la Oficina de Seguridad de la Información y tenga su aprobación.

- **Campo Observaciones:** se debe incluir la información de seguimiento frente al avance del plan de tratamiento de acuerdo a su estado.

g. Si el usuario desea pasar del estado “Definido” al estado “Aprobado” el sistema le permitirá al usuario visualizar el siguiente avance del plan de tratamiento:

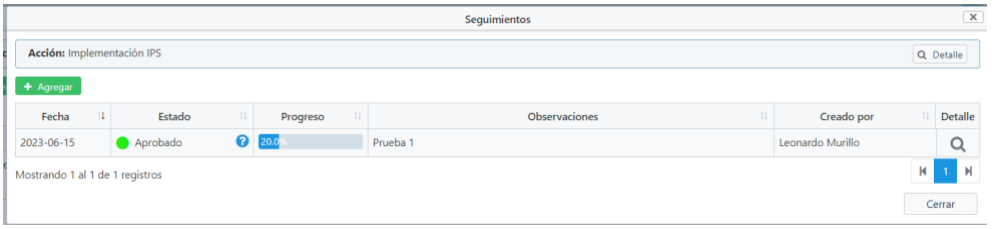


Ilustración 67. Ventana de seguimiento planes de tratamiento “Aprobado”

Si el usuario desea pasar del estado “Aprobado” al estado “Iniciado” el sistema le permitirá al usuario visualizar el siguiente avance del plan de tratamiento:

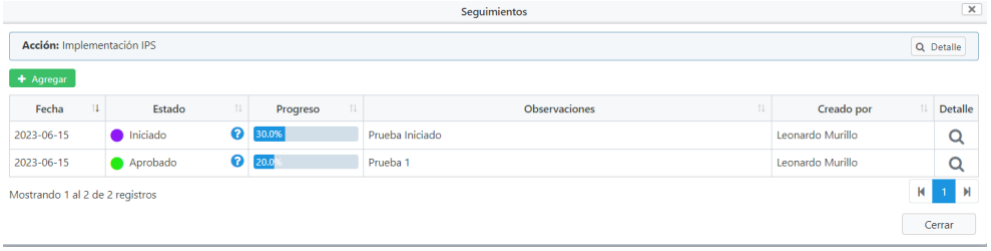


Ilustración 68. Ventana de seguimiento planes de tratamiento “Iniciado”

Si el usuario desea pasar del estado “Iniciado” al estado “En ejecución” el sistema le permitirá al usuario visualizar el siguiente avance del plan de tratamiento:

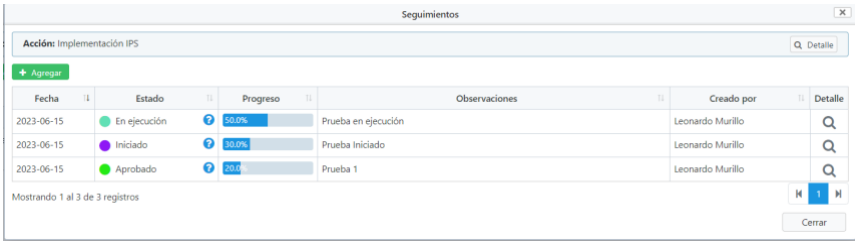


Ilustración 69. Ventana de seguimiento planes de tratamiento “En ejecución”

Si el usuario desea pasar del estado “En ejecución” al estado “Finalizado” el sistema le permitirá al usuario visualizar el siguiente avance del plan de tratamiento:

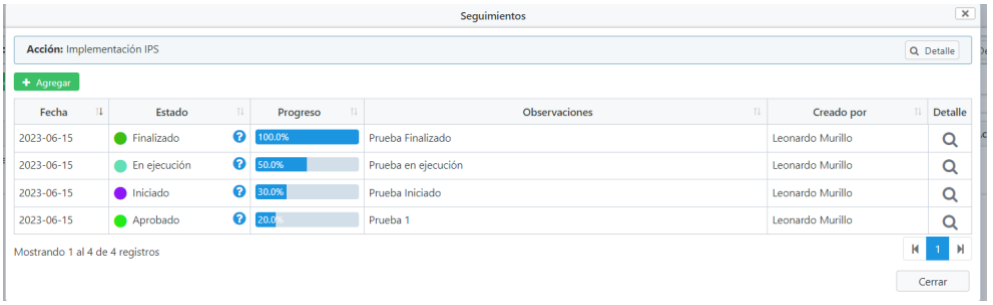


Ilustración 70. Ventana de seguimiento planes de tratamiento “Finalizado”

Una vez se llegue al estado “Finalizado” el sistema no permitirá realizar más seguimientos sobre al plan de tratamiento.

> **Nota:** si el plan de tratamiento tiene como objetivos mejorar la implementación de un control, se debe realizar nuevamente la evaluación de dicho control como se especifica en el numeral *3.7.1.1. Evaluación de controles* y actualizar los campos necesarios para reflejar la situación reciente.

3.10 Reporte del plan de tratamiento de riesgos de seguridad de la información

La herramienta GRC, contiene una opción en el módulo de riesgos para generar el reporte del plan de Tratamiento de Riesgos.

En este reporte, además de las columnas que se manejan en el módulo de planes, le permite al usuario observar el valor de otras columnas de interés que se diligenciaron en el Módulo de Riesgos. Para generar este reporte el usuario debe:

a. Ingresar por el Módulo de Riesgos – Reportes

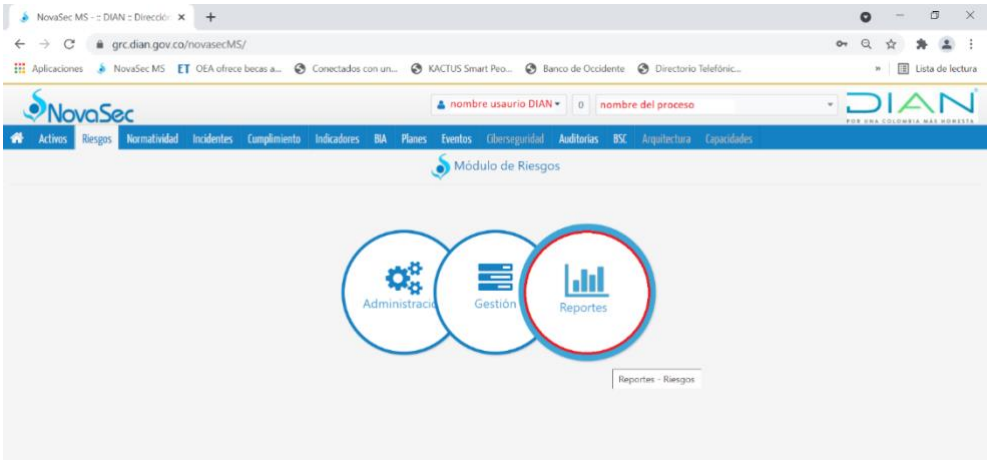


Ilustración 71. Menú riesgos, opción "reportes"

b. Escoger la opción "Generador de plan de tratamiento"

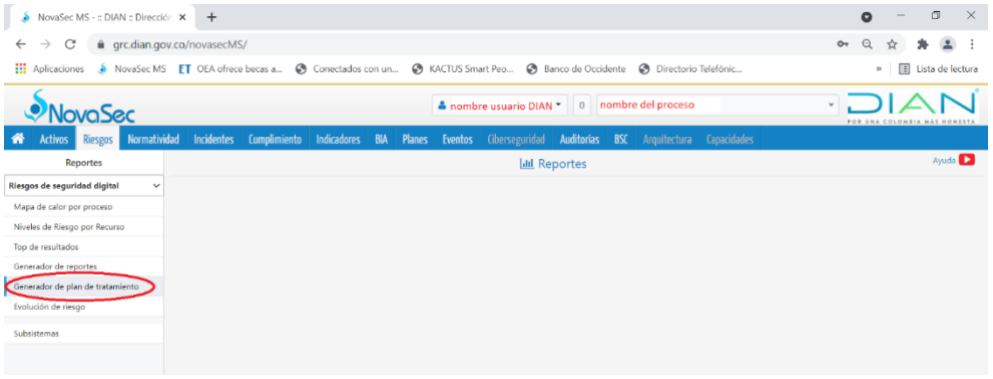


Ilustración 72. Menú riesgos, opción de generación de reportes

c. Dar clic en el botón "Agregar" y diligenciar los siguientes campos

- Nombre: diligenciar el nombre del plan de tratamiento de riesgos
- Descripción: diligenciar la descripción del plan de tratamiento de riesgos
- Tipo de Reporte: escoger Tabular: Riesgo – Control – Plan
- Procesos
- Escoger el proceso y pasar a la zona de la derecha

  NOTA: para generar el Plan de Tratamiento de Riesgos de seguridad de la información, escoger todos los procesos.
- Columnas del riesgo

En la zona de la izquierda marcar las columnas:

✓ Probabilidad riesgo residual

- ✓ Impacto riesgo residual
- ✓ Riesgo residual
- ✓ Nivel de tratamiento

Y dar clic en el ícono para pasarlas a la zona derecha.

- Columnas del control

En la zona de la izquierda marcar las columnas:

- ✓ Responsable de diseño
- ✓ Responsable de implementación
- ✓ Tipo de control
- ✓ Observaciones de implementación
- ✓ Diseño – Calificación Diseño
- ✓ Implementación – Calificación Implementación
- ✓ Efectividad – Calificación Efectividad
- ✓

Y dar clic en el ícono para pasarlas a la zona derecha

- Estado del plan

  En la zona de la izquierda marcar la columna:

  - ✓ Activo

  Y dar clic en el ícono para pasarlas a la zona derecha.

  Para el ejemplo, los campos quedarían como se muestra en la siguiente imagen. Dar clic en “Guardar

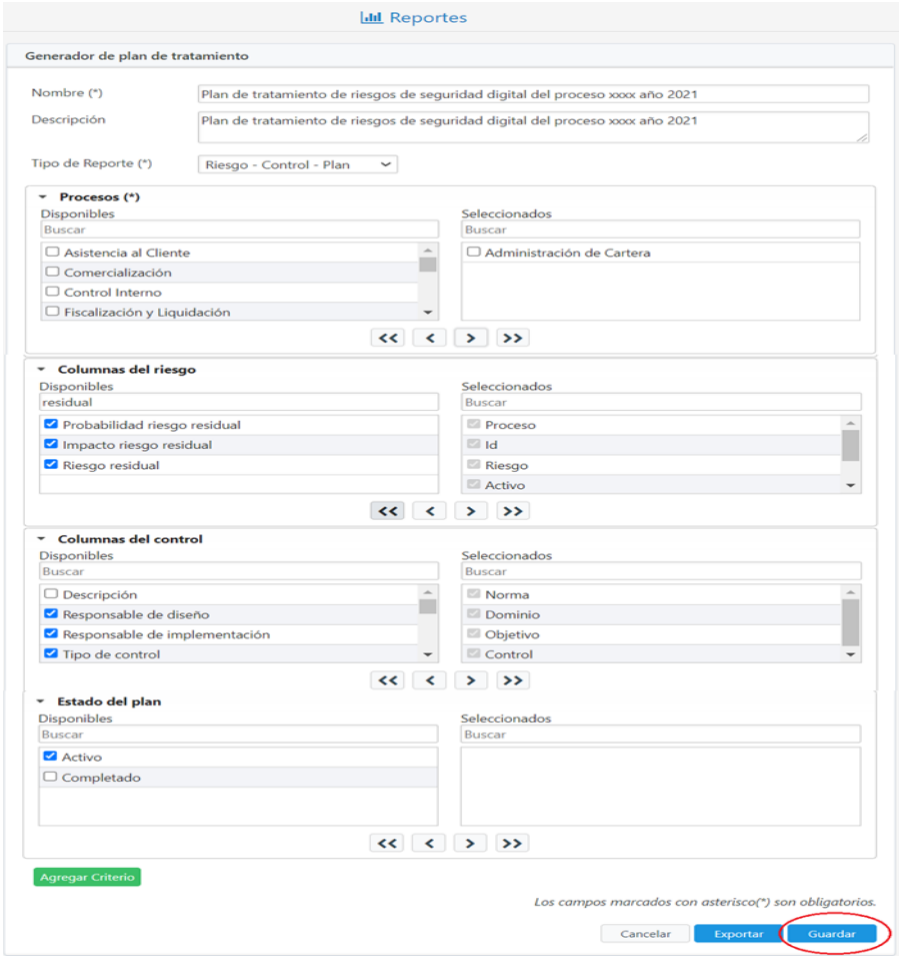


Ilustración 73. Ventana de selección campos de reportes

d. En la pantalla de reportes dar clic en el ícono de Exportar 

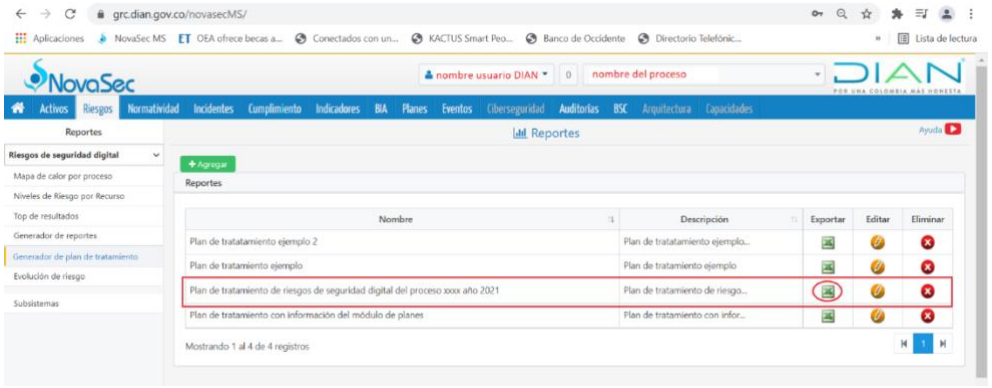


Ilustración 74. Ventana de generación de reporte en “Excel”

e. Si aparece el siguiente mensaje, dar clic en “Sí”:

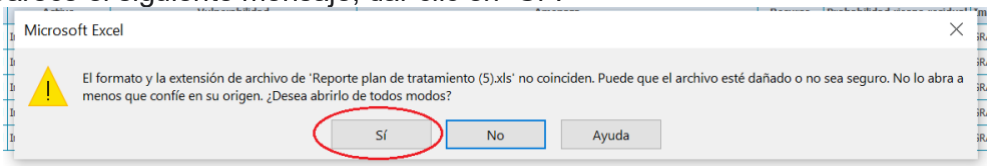


Ilustración 75. Ventana aprobación de generación del reporte

f. Se genera un archivo Excel con la información solicitada:

3.11 Reporte del plan de Tratamiento de Riesgos de seguridad digital en el Módulo de Planes (con tareas detalladas)

Para generar el reporte en el módulo de planes, que permite ver el avance de cada una de las tareas:

a. Ingresar al Módulo de Planes – Reportes

Ilustración 76. Menú planes, opción reportes

b. Escoger la opción “Generador de Reportes”. Diligenciar los campos Nombre y Descripción y pasar todos los campos del panel de la izquierda al panel de la derecha, de las zonas “Columnas del Plan” y “Columnas de Tareas” con el botón . Dar clic en “Guardar”.

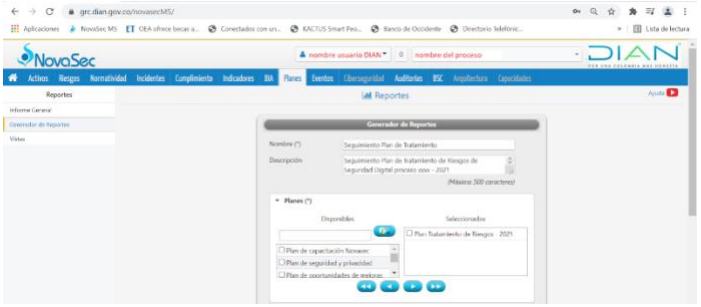


Ilustración 77. Ventana de selección campos de reportes

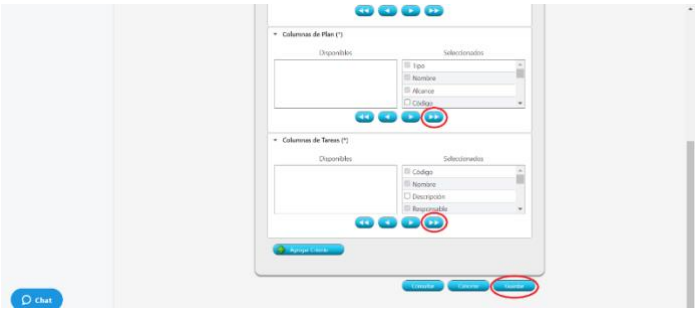


Ilustración 78. Ventana de selección campos de reportes

c. Dar clic en “Consultar” al reporte de Seguimiento, recién creado

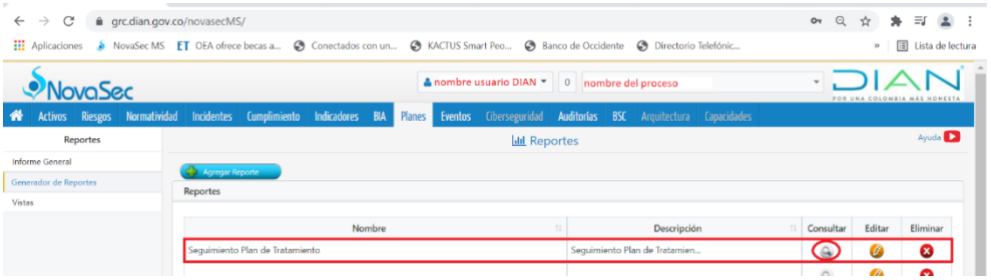


Ilustración 79. Ventana de generación de reportes

d. Dar clic en el ícono de Excel

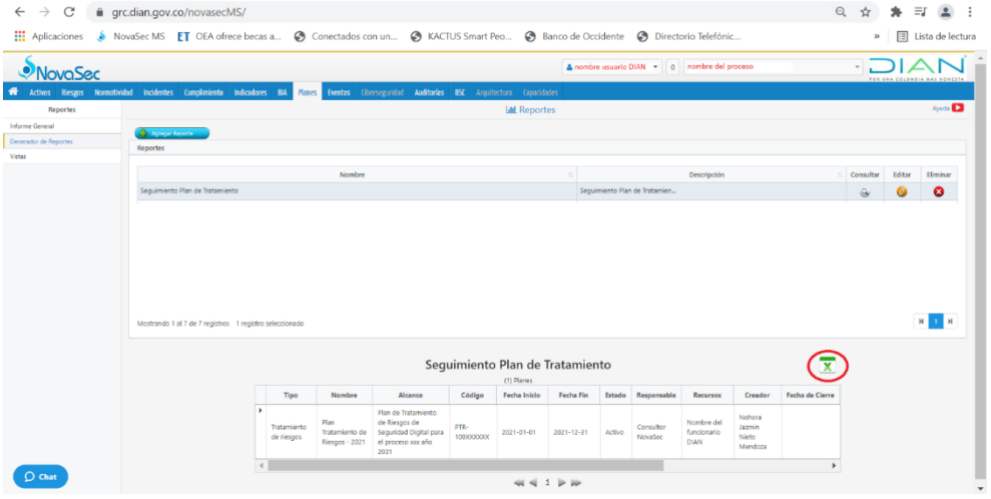


Ilustración 80. Ventana de selección campos de reportes “Excel”

e. El archivo generado muestra cada una de las tareas con su avance:

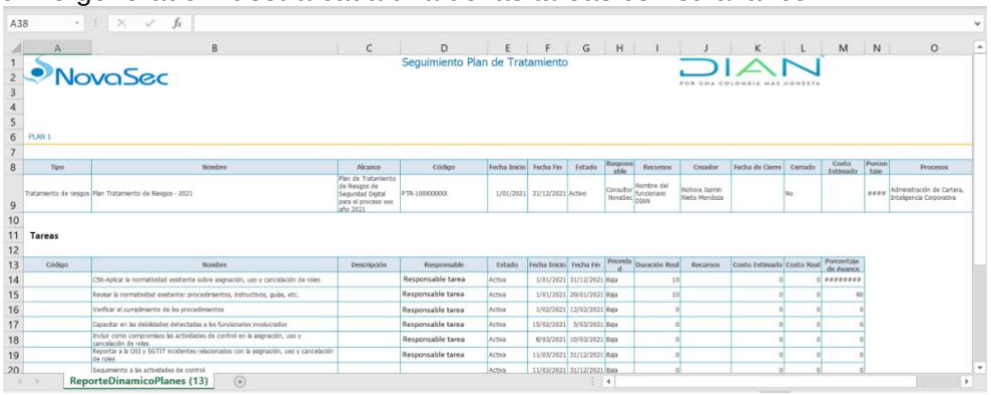


Ilustración 81. Visualización de reportes en "Excel"

3.12 Aprobación del riesgo de seguridad de la información

La aprobación de un riesgo se puede realizar en cualquiera de los módulos; Identificación, Valoración o Tratamiento. Esta aprobación la debe realizar el superior jerárquico o líder del proceso quien debe contar con permisos especiales en el GRC, los cuales deben haber sido configurados previamente.

Se recomienda realizar la aprobación luego de la etapa de "Valoración". Es importante tener en cuenta que los **riesgos aprobados** ya no se pueden modificar, ni eliminar.

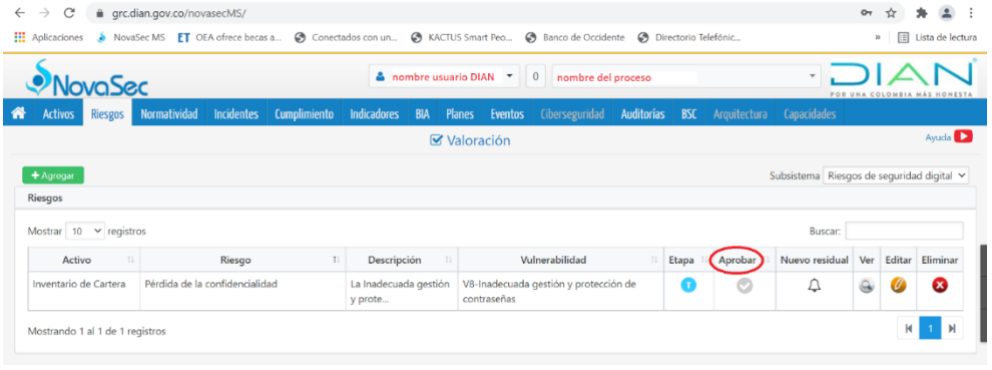


Ilustración 82. Opción de aprobación de los riesgos

Los posibles estados de aprobación que puede tener un riesgo son los siguientes:

Ilustración 83. Estado de aprobación de riesgos

- Si la columna "*Aprobado"* está vacía indica que el riesgo aún no se puede aprobar.
- Si la columna "*Aprobado* se muestra con un ícono en color verde indica que el riesgo está aprobado. Al hacer clic sobre el botón su estado cambia automáticamente a No Aprobado .

Si la columna *Aprobado* se muestra con un ícono en color gris indica que el riesgo aún no se ha aprobado. Al hacer clic sobre el botón , su estado cambia automáticamente a Aprobado .

4 CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de cambios	Tipo de información
	Desde	Hasta		
1	13/09/2022	06/12/2023	Versión inicial manual del usuario para el registro de la gestión de riesgos de seguridad digital de la DIAN	Esta versión Corresponde a Información Pública
2	07/12/2023		Se incluyen ajustes derivados del cambio de la metodología para la gestión de riesgos de seguridad de la información Elimina los anexos: Anexo 1 - Tabla de Vulnerabilidades Anexo 2 – Amenazas Anexo 3 - Ejemplos de Amenazas para Activos de Información Anexo 4 - Controles Anexo A NTC-ISO/IEC 27001:2013	Esta versión corresponde a información Pública

Elaboró:	Consultor Externo EY **Elaboración técnica**	Consultor	Oficina de Seguridad de la Información
	Alfredo Ahumada Ahumada	Gestor II	Coordinación de Procesos y

	Elaboración metodológica		Riesgos Operacionales
	Tito Alejandro Menjura Murcia **Elaboración metodológica**	Gestor II	Coordinación de Procesos y Riesgos Operacionales
Revisó:	Carlos Javier Ibañez Serna	Gestor II	Oficina de Seguridad de la Información
Aprobó:	Hugo Alcides Pérez Pinilla	Jefe de Oficina (E)	Oficina de Seguridad de la Información