

Contenido

1. Introducción.....	2
2. Análisis de Activos.....	2
3. Análisis de controles	4
4. Categorización amenazas.....	9
5. Análisis de Riesgos.	10
6. Plan de tratamiento de riesgos.....	14
7. Análisis de los Incidentes de Seguridad.....	16
8. Conclusiones	17
9. Bibliografía	17

1. Introducción

El objetivo de este documento es presentar el nivel de control actual realizado una preauditoria del nivel de cumplimiento de gestión de la seguridad de la compañía Protección S.A en la plataforma eMarisma. Protección es una empresa Colombiana de Pensiones, inversiones y Cesantías que aporta un poco más del 10% del PIB de Colombia. Su visión es ser el principal aliado de sus clientes en la construcción y gestión de su patrimonio, y su misional es proteger, desde el presente, el futuro de sus clientes en la construcción de su patrimonio y generarles valor a sus afiliados para el cumplimiento de sus metas.

2. Análisis de Activos

Tabla 1. Activos seleccionados de la compañía Protección S.A

Tipo	Nombre	Valor Estratégico
[D] Datos / Información	Base de datos cuentas de Afiliados	Muy Alto
[D] Datos / Información	Base de datos de inversiones	Muy Alto
[D] Datos / Información	Base de datos empleados	Muy Alto
[keys] Claves criptográficas	Certificados de seguridad SSL	Medio
[HW] Equipos informáticos (hardware)	Circuito cerrado de vigilancia	Bajo
[SW] Aplicaciones (software)	Código fuente	Muy Alto
[HW] Equipos informáticos (hardware)	Computadores	Bajo
[Media] Soportes de información	Contratos	Alto
[COM] Redes de comunicaciones	equipos de red	Muy Bajo
[D] Datos / Información	Información jurídica	Muy Alto
[L] Instalaciones	Inmuebles de la Dirección general	Muy Bajo
[SW] Aplicaciones (software)	Página Web de Protección	Alto
[P] Personal	Personal Protección	Medio
[Media] Soportes de información	Repositorio Filenet	Muy Alto
[S] Servicios	Servicios Cloud	Muy Alto

En la gráfica anterior se observan los 15 Activos que se tomaron de la compañía Protección S.A alojadas en la dirección general, se seleccionaron activos de diferentes tipos, desde activos de tipo información hasta inmuebles de la empresa. La distribución de los activos por el tipo se ve en la siguiente gráfica:

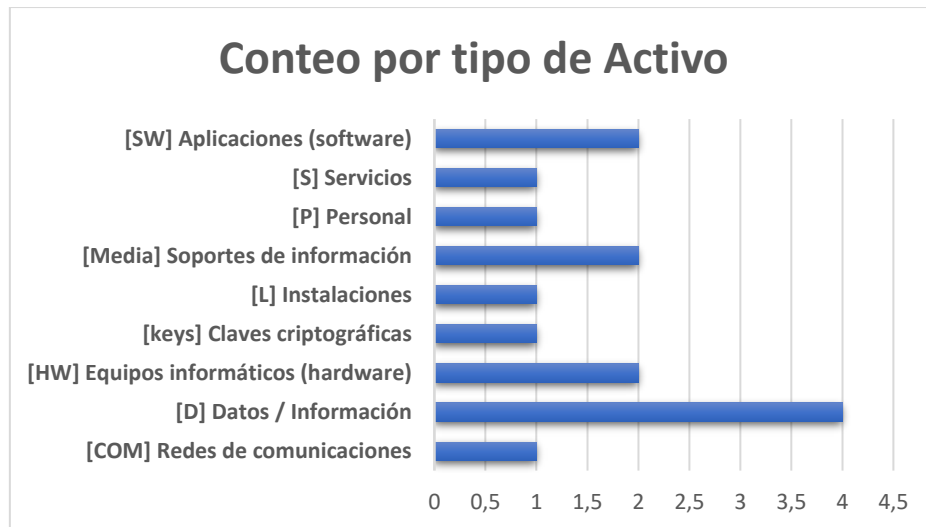


Ilustración 1. Conteo de activos según tipo de datos

Dónde se puede observar que la mayoría de los activos que se tienen son digitales como bases de datos de información de la empresa, repositorios documentales de la empresa y aplicaciones de software. En la siguiente Gráfica veremos que la mayoría de los activos seleccionados son de nivel estratégico y que a su vez la mayoría de los activos digitales representan el valor estratégico más importante para la compañía, ya que por ejemplo vulnerabilidades en la información de un afiliado pueden acarrear temas jurídicos hacia la empresa y sanciones económicas.

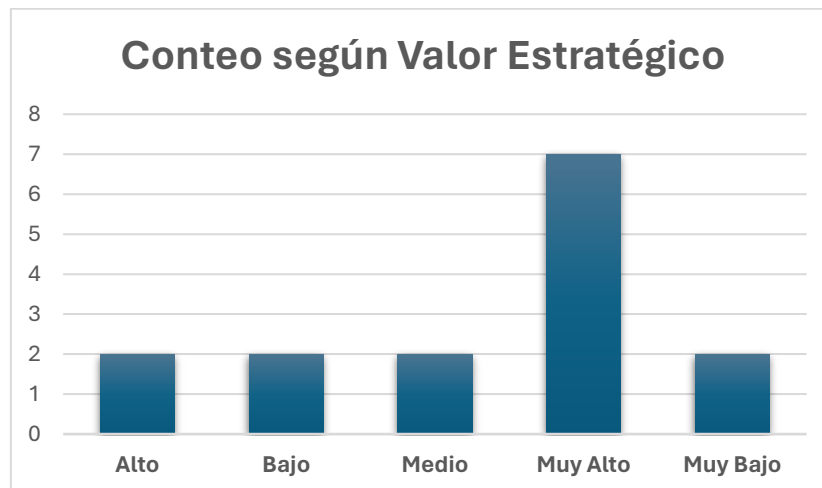


Ilustración 2. Conteo de activos según valor estratégico.

3. Análisis de controles

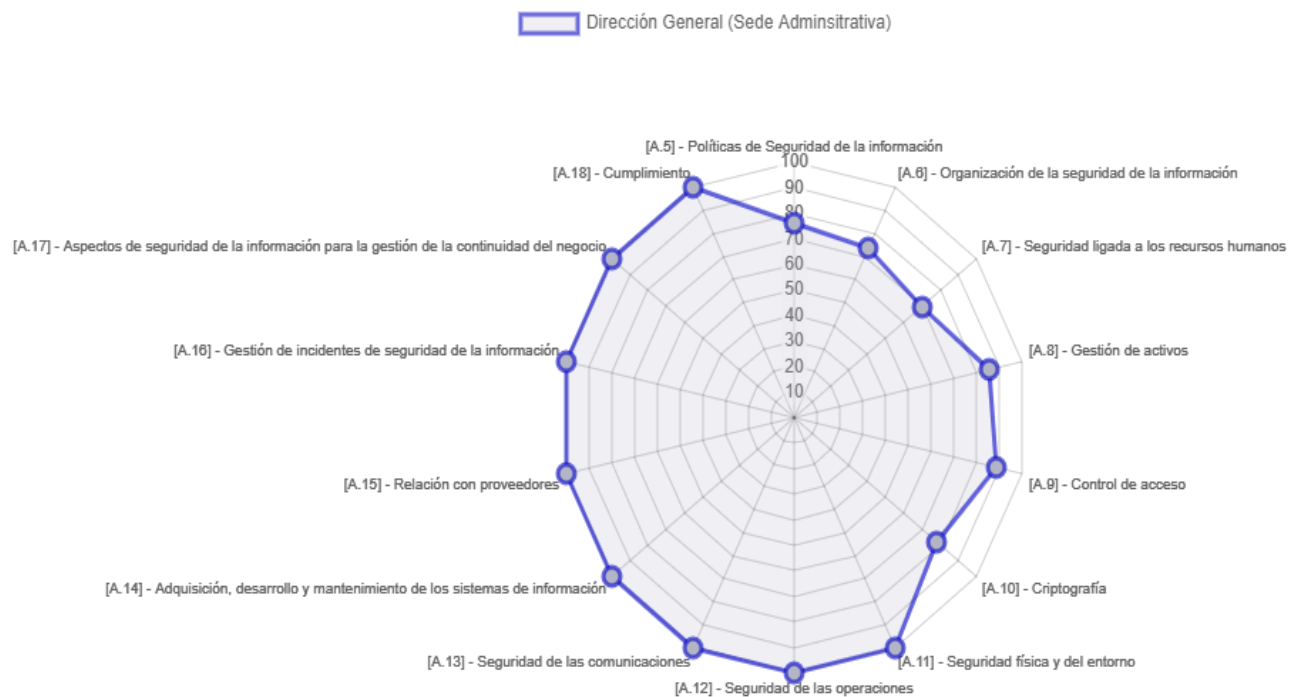


Ilustración 3. Nivel de cumplimiento según Dominio

De la ilustración 3 se observa que el dominio A7 Seguridad ligada a los recursos humanos es el dominio con más oportunidades de mejora dentro de la compañía y el dominio A9 es nuestro dominio con mayor nivel de cumplimiento, lo ideal sería enfocar los esfuerzos en aumentar el nivel de cumplimiento en nuestro eslabón más débil sin descuidar los que tienen un nivel de cumplimiento mayor. En Las siguientes figuras veremos cada dominio a nivel de subdominios para tener un panorama más claro de los subdominios a los que debemos abordar con más prioridad.

Diagramas de Cobertura

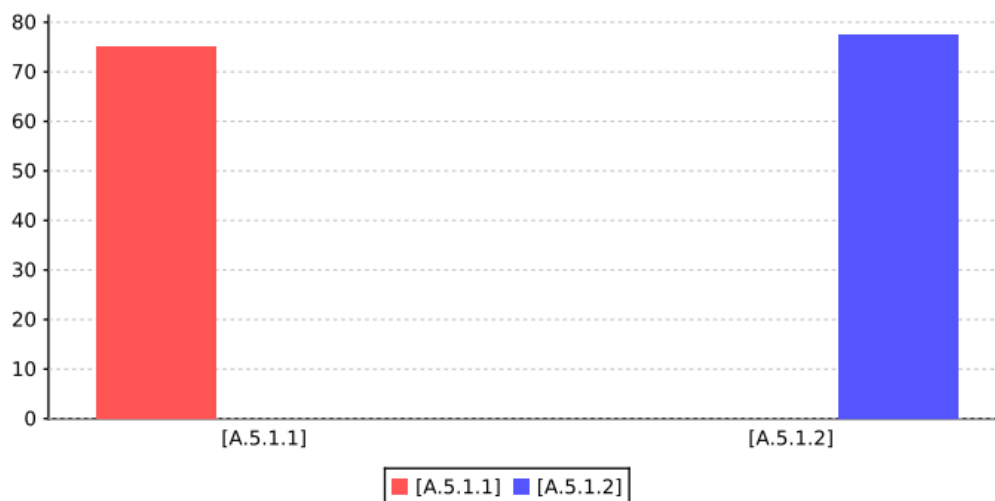


Ilustración 4. Comportamiento a nivel de subdominios del dominio A5.

En el dominio A5 vemos que se tiene un balance a nivel de subdominios y están en un promedio de 75% de cumplimiento, todavía hay oportunidades de mejora en cuánto a la divulgación de las políticas de seguridad a los nuevos usuarios, para segmentar estas capacitaciones por cargos. Además, se podría aplicar a la revisión gerencial el hecho de tener cronogramas definidos y ser más eficientes en las nuevas políticas de seguridad.

Diagramas de Cobertura

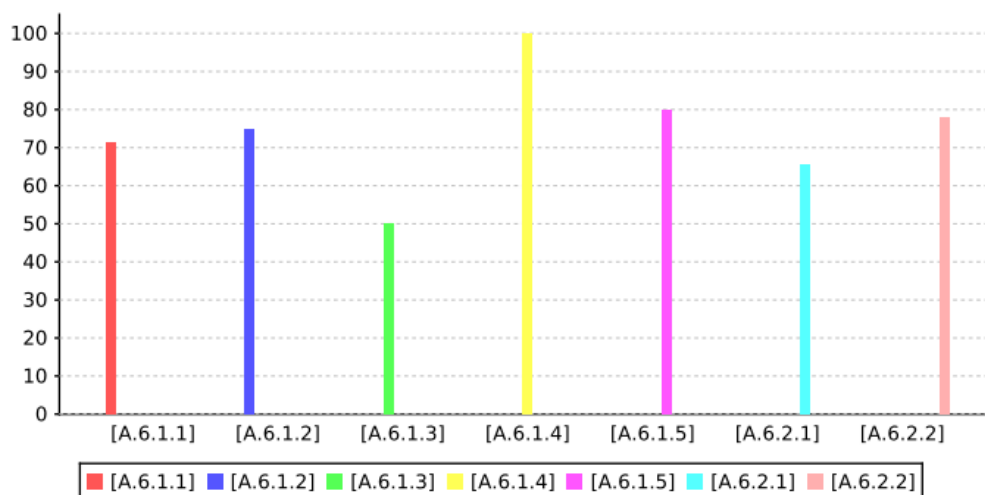


Ilustración 5. Comportamiento a nivel de subdominios del dominio A6.

En el dominio A6 vemos que se tiene algunos subdominios con falencias notorias como el subdominio A6.1.3 Contacto con las autoridades de control dónde hay oportunidades en la estandarización de estas comunicaciones ya que se tiene el proceso definido pero no un documento guía para realizar la notificación Y EL A6.2.1 Política de dispositivos móviles ya que

no hay una correcta divulgación de la información de los riesgos y requerimientos a los usuarios que usan los aplicativos de la empresa desde sus dispositivos móviles.

Diagramas de Cobertura

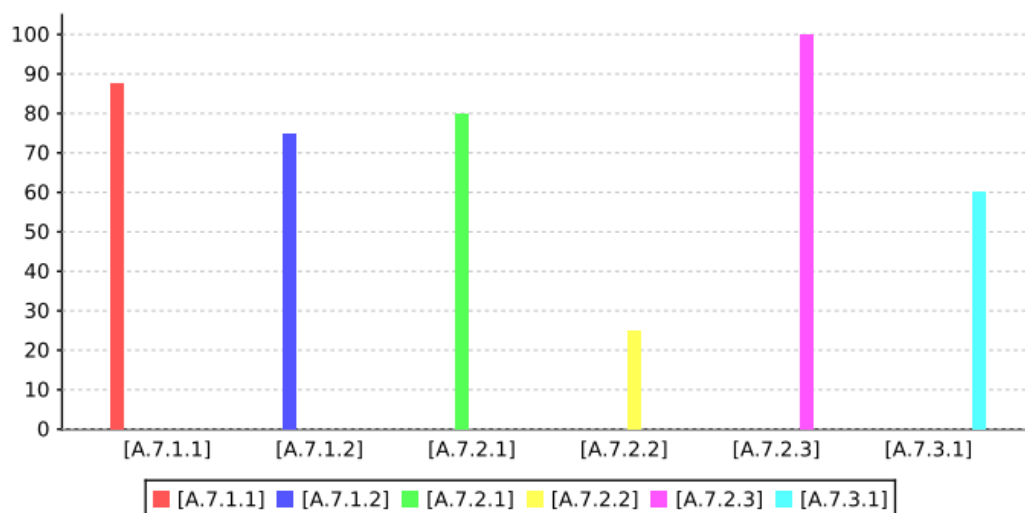


Ilustración 6. Comportamiento a nivel de subdominios del dominio A7.

En el dominio A7 vemos que se tiene algunos subdominios con falencias notorias como el subdominio A7.2.2 Concienciación, educación y capacitación en seguridad de la información, dónde se debe enfocar los esfuerzos en brindar una correcta capacitación a los usuarios externos en el correcto uso de las instalaciones de procesamiento de información, haciendo campañas cursos y documentación clara para estos usuarios A7.3.1 Responsabilidades ante la finalización o cambio, No hay políticas de tiempo para seguir cumpliendo responsabilidades para los usuarios que finalizan su vinculación laboral, además los procesos de terminación o cambio de cargo no se tienen correctamente estructurados porque en algunas ocasiones se generan reprocesos y confusiones, por lo que se debe atacar este proceso con herramientas de BPM dónde cada uno de los actores sepa cuando actuar en cada caso que se presente.

Diagramas de Cobertura

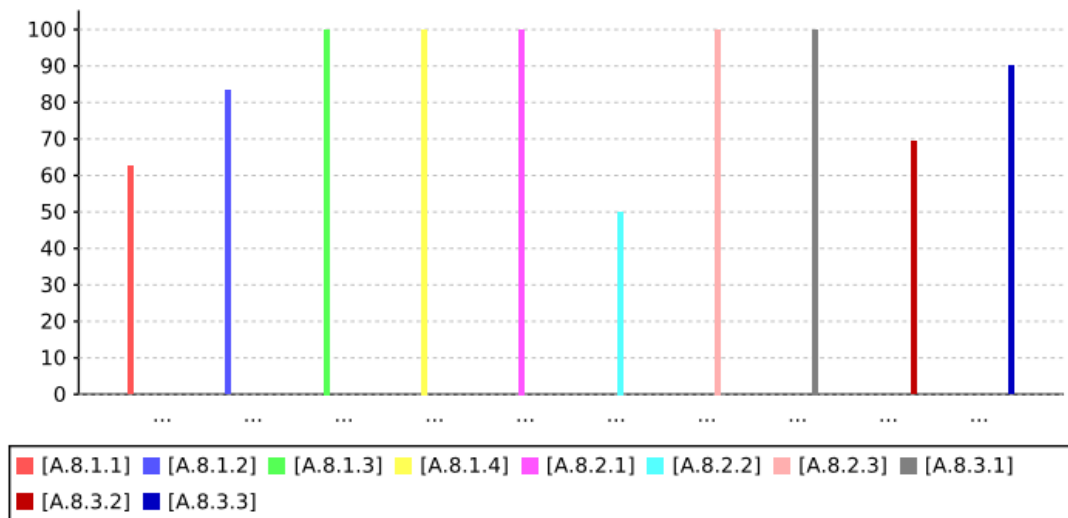


Ilustración 7. Comportamiento a nivel de subdominios del dominio A8.

En el dominio A8 vemos que se tiene algunos subdominios con falencias notorias como el subdominio A8.2.2 Etiquetado de la información, ya que no toda la información que se administra en Protección está correctamente clasificada y rotulada, se debe continuar revisando en las auditorías que con el tiempo cada vez sea menos la información sin rotular y clasificar EL A8.1.1 Responsabilidad sobre los activos , dónde se debe fortalecer los procesos de control de inventarios y realizar reportes periódicos del status de los inventarios, además de jornadas periódicas de actualización.

Diagramas de Cobertura

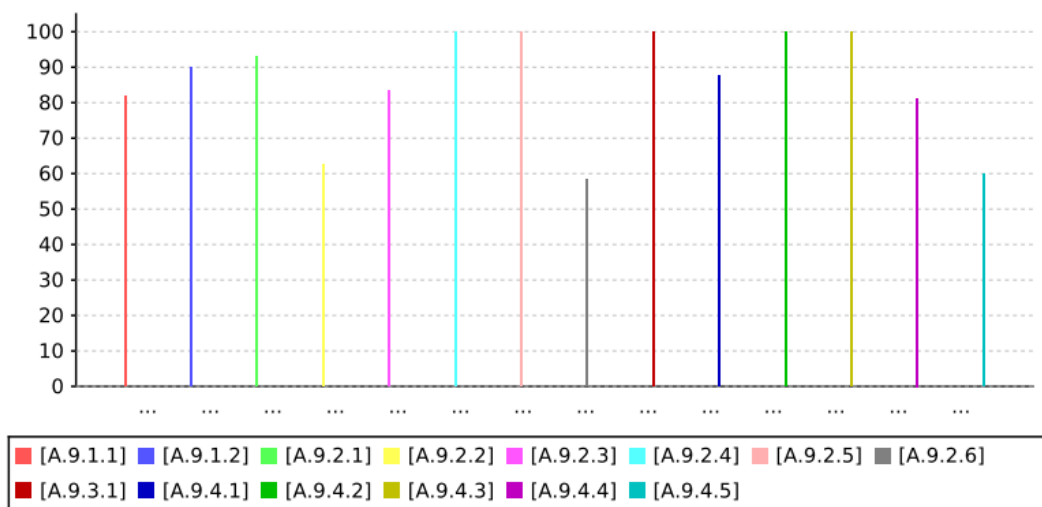


Ilustración 8. Comportamiento a nivel de subdominios del dominio A9.

En el dominio A9 vemos que se tiene algunos subdominios con falencias notorias como el subdominio A9.2.6 Retirada o reasignación de los derechos de acceso, dónde hay oportunidades de eliminación o cambio de claves automáticas cuándo algún usuario se elimine, sobre todo las falencias se tienen con los usuarios externos por lo que se debería contemplar un proceso automático que lo realice, EL A9.4.5 Control de acceso al código fuente de los programas ya que algunos usuarios administradores que deberían poder acceder a los repositorios del personal de TI no tienen acceso y se tiene el mismo repositorio para códigos en desarrollo, test y producción, se debería separar los repositorios por ambiente. También en el subdominio A9.2.2. Provisión de acceso de usuario, se tienen falencias en la comunicación de los derechos y deberes cuando un usuario ingresa nuevo, no se firman declaraciones y las políticas en el contrato no están estipuladas claramente. Se debe verificar con el área jurídica para cambiar estos contratos y en caso de brindarle información a algún usuario a información sensible generar un documento o un “otro sí” para blindarse de alguna forma jurídicamente.

Diagramas de Cobertura

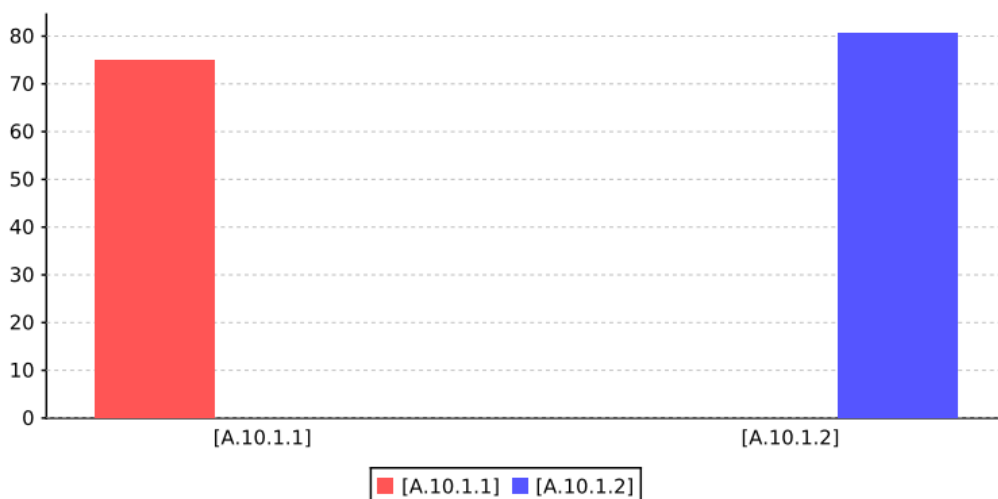


Ilustración 9. Comportamiento a nivel de subdominios del dominio A10.

En el dominio A10 vemos que se tiene un balance a nivel de subdominios y están en un promedio de 75% de cumplimiento, todavía hay oportunidades de mejora en cuánto a la divulgación, custodia y procedimientos para las claves criptográficas. Se debería construir una guía donde se abarquen todos estos factores y así mejorar los niveles de cumplimiento de este dominio.

ANÁLISIS DEL SOA

El patrón usado es el SNT_08_001 - Patrón General 2013. En Protección Se tienen diferentes responsables dentro de cada dominio lo que demuestra que la seguridad de la información hace parte integral de la compañía, estos responsables son de cada área de la compañía desde el personal directivo, personal administrativo, personal de TI, personal de ciberseguridad y personal de recursos humanos. Todos los dominios y subdominios aplican para la auditoría. El

análisis de auditoría debería enfocarse en la siguiente tabla que representa el resumen de los controles a nivel de dominio para realizar una correcta priorización.

Tabla 2 Resumen de calificación de preauditoría a nivel de dominios.

Dominio	Calificación
[A.5] - Políticas de Seguridad de la información	76.24%
[A.6] - Organización de la seguridad de la información	73.49%
[A.7] - Seguridad ligada a los recursos humanos	69.86%
[A.8] - Gestión de activos	85.4%
[A.9] - Control de acceso	88.62%
[A.10] - Criptografía	77.77%

4. Categorización amenazas

Tabla 3. Reporte amenazas

Nombre Amenaza	Probabilidad Ocurrencia	Porcentaje Degradación
Repudio	Muy Bajo (20.0%)	Muy Alto (100.0%)
Interceptación de información (escucha)	Medio (60.0%)	Muy Alto (100.0%)
Modificación deliberada de la información	Bajo (40.0%)	Muy Alto (100.0%)
Destrucción de información	Bajo (40.0%)	Muy Alto (100.0%)
Manipulación de los equipos	Medio (60.0%)	Medio (60.0%)
Acceso no autorizado	Muy Bajo (20.0%)	Bajo (40.0%)
Análisis de tráfico	Medio (60.0%)	Alto (80.0%)
Divulgación de información	Medio (60.0%)	Alto (80.0%)
Alteración de secuencia	Bajo (40.0%)	Alto (80.0%)
Manipulación de programas	Alto (80.0%)	Alto (80.0%)

Decidimos analizar las primeras 10 amenazas que nos generaba la herramienta, y podemos observar de la Tabla 3 que las amenazas que seleccionamos en su mayoría tienen una

probabilidad de ocurrencia media o baja, dónde resaltamos la manipulación de programas como una amenaza que tiene una alta probabilidad de ocurrir dada la cantidad de aplicativos que se manejan en Protección y el difícil seguimiento sobre estos, a pesar de tener controles de registro y auditorías, además muchas de las operaciones se realizan manualmente sobre estos aplicativos, por lo que hay alta probabilidad de encontrarse con una persona malintencionada con los permisos y exceso de confianza sobre las personas. Algo importante del reporte de amenazas es que la mayoría de las amenazas mencionadas tienen un porcentaje de degradación alto ya que en su mayoría tienen alguna relación directa o indirecta con la información de la empresa o de sus aplicativos, y el activo más importante dentro de una compañía de pensiones son los datos ya que hay información de rendimientos de sus cuentas, información de la historia laboral de un empleado e información personal de los millones de afiliados que tiene Protección.

5. Análisis de Riesgos.

Tabla 4 Resultado Riesgos

Nombre Activo	Nombre Amenaza	Va	Fr	V	[C]	[D]	[I]	IT	IMP	Ries	Ries	VRR
Base de datos de inversiones	Fugas de información	5	20.0	9.87641	100	20	20	100.0	500.0	250.0	24.691	5.0
Página Web de Protección	Acceso no autorizado	4	20.0	10.607	90	20	90	90.0	360.0	216.0	22.9111	5.0
Base de datos cuentas de Afiliados	Modificación deliberada de la info	5	40.0	8.12452	70	50	100	100.0	500.0	200.0	16.249	4.0
Información jurídica	Acceso no autorizado	5	20.0	10.607	100	20	50	100.0	500.0	200.0	21.214	4.0
Base de datos de inversiones	Acceso no autorizado	5	20.0	10.607	100	20	50	100.0	500.0	100.0	10.607	3.0
Personal Protección	Extorsión	3	20.0	5.86957	80	50	80	80.0	240.0	120.0	7.04348	3.0
Servicios Cloud	Uso no previsto	5	20.0	10.4857	20	20	20	20.0	100.0	20.0	2.09715	1.0
Contratos	Errores del administrador	4	20.0	5.49837	20	20	20	20.0	80.0	16.0	0.87973	0.0
Inmuebles de la Dirección general	Ataque destructivo	1	20.0	1.2931	5	50	5	20.0	20.0	10	0.129	0.0
Servicios Cloud	Alteración de secuencia	5	40.0	0.0	10	60	80	80.0	400.0	160.0	0.0	0.0

De la tabla 4 podemos observar que el puntaje máximo que obtuvimos del análisis de riesgo fue de 5 en el valor de riesgo residual, lo cual tiene sentido porque dentro de todo es una empresa con buenos controles relacionados a la ciberseguridad por los activos tan delicados que maneja referente a los afiliados a pensiones, cesantías e inversiones. Uno de los activos que presentó mayor valor de riesgo residual fue el de la base de datos de inversiones antes una amenaza de fuga de información esto tiene mucho sentido ya que es un activo de mucho valor y afecta directamente en un 100% el valor de la confidencialidad, la información en la empresa es el activo más importante además que en esta base de datos se tiene toda la estrategia de la compañía de cara a ser competitiva frente a las otras empresas. Otro ejemplo interesante es el de la amenaza de extorsión a personal de protección que, a pesar de no tener una frecuencia de pasar muy alta, si pudiese tener una afectación grande tanto a la integridad de la información como a la confidencialidad y un poco a la disponibilidad, porque se podría hacer que empleados modifiquen información de base de datos o revelen información específica de la empresa. Un ataque destructivo hacia los inmuebles de la organización no tiene mucha probabilidad de

ocurrir además que el activo casi no representa valor para la empresa por eso se le pone un valor de riesgo residual de cero.

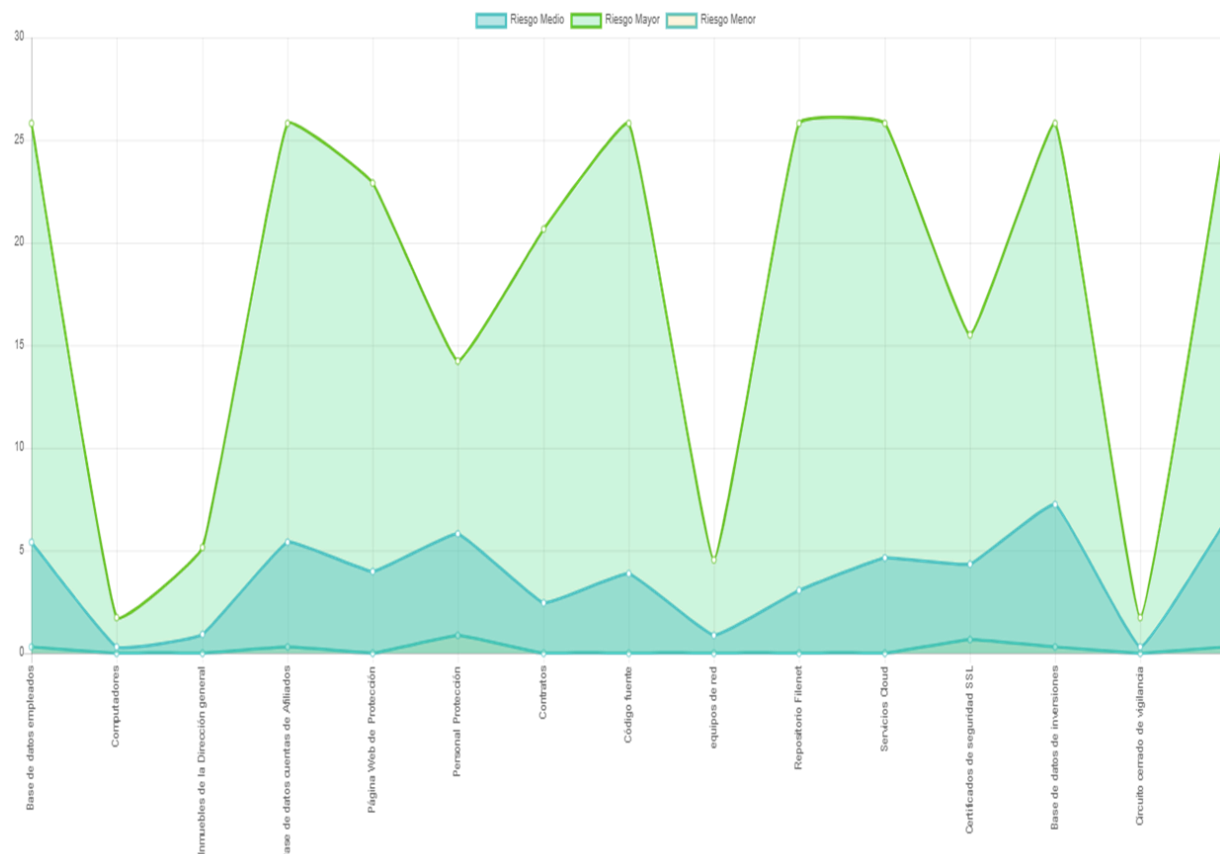


Ilustración 10

De la gráfica anterior podemos observar que los computadores, inmuebles, equipos de red y los circuitos cerrados de vigilancia representan activos con poco riesgo tanto medio, bajo o alto; En comparación con activos como la información jurídica, base de datos de afiliados, empleados y de inversiones, códigos fuentes y repositorios de documentación (Filenet), los cuales tienen un mayor riesgo. Adicional cabe resaltar que el Personal de Protección tiene una importancia alta en el riesgo normalmente debido a temas como la fuga de información e ingeniería social,

aunque estos se mitigan con capacitaciones y formaciones, siempre será un factor importante para considerar durante el análisis de riesgo.

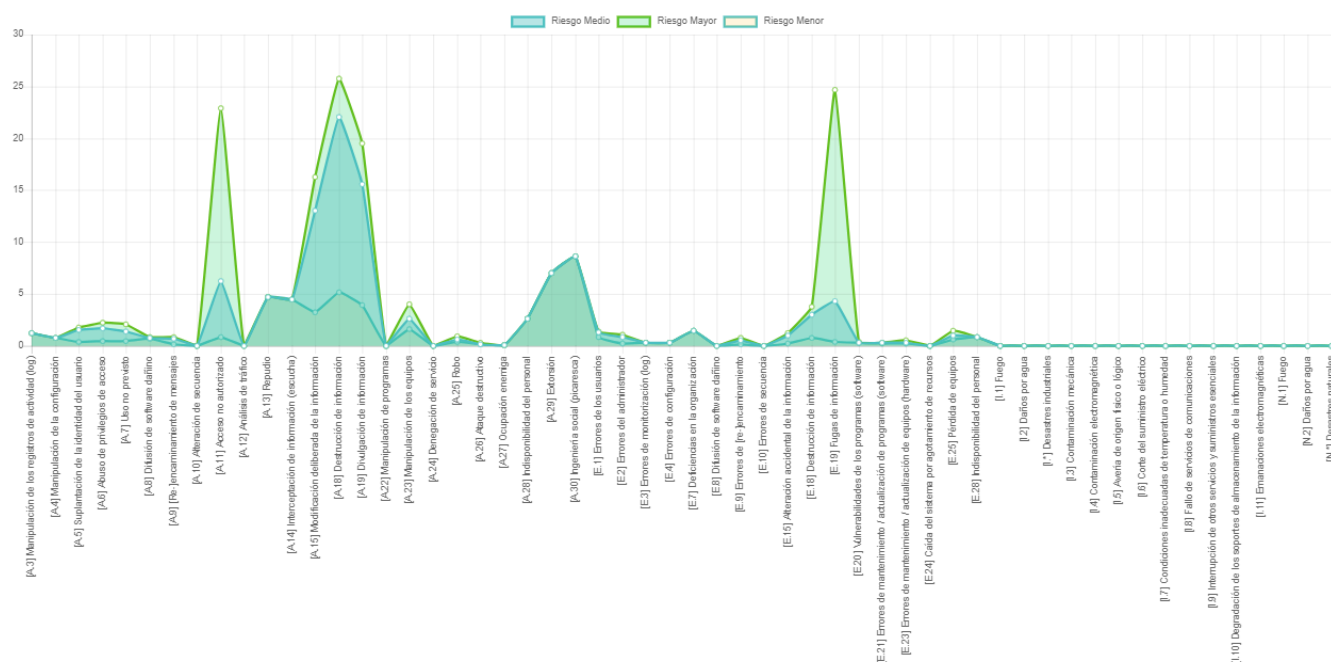


Ilustración 11

En la gráfica anterior podemos observar los puntajes de riesgo por amenazas que pueden ocurrir dentro de la compañía, se puede inferir por la gráfica que las variables modificación, interceptación, destrucción, fugas y divulgación deliberada de la información, son lo que presentan un mayor riesgo de presentarse, en caso de ocurrir presentan una mayor amenaza a la integridad de la información. Los demás riesgos tienen una probabilidad de ocurrencia mucho mejor y a su vez un impacto bajo. Definitivamente los planes de control que se realicen deben tener como prioridad el disminuir el riesgo de accesos no autorizados y fugas de información ya que la información es el activo más importante dentro de una compañía de pensiones y cesantías, donde una materialización de una amenaza de las mencionadas podría provocar daños a la reputación de la compañía, demandas y procesos jurídicos en contra de Protección S.A y pérdidas económicas a los rendimientos de los afiliados.

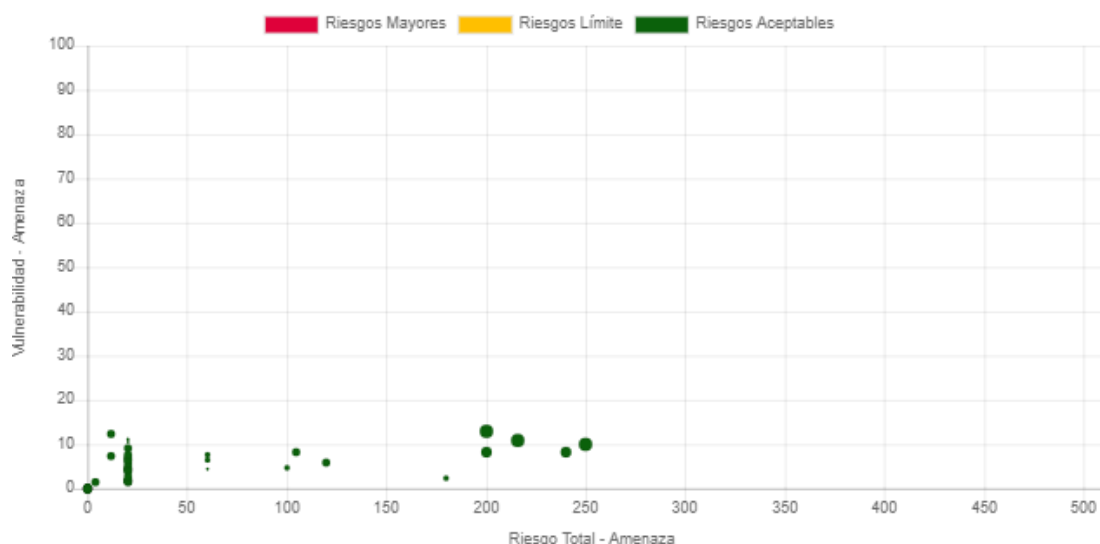


Ilustración 12

Como se observa en la gráfica 12 los riesgos presentados por la compañía provienen todos de riesgos aceptables, pero se debe prestar mucha atención a las que tienen un puntaje de riesgo elevado porque a pesar de estar en la zona aceptable también por descuido en las políticas podrían acceder a la zona límite por lo cual se debe seguir controlando y monitoreando los niveles de riesgo de las amenazas.

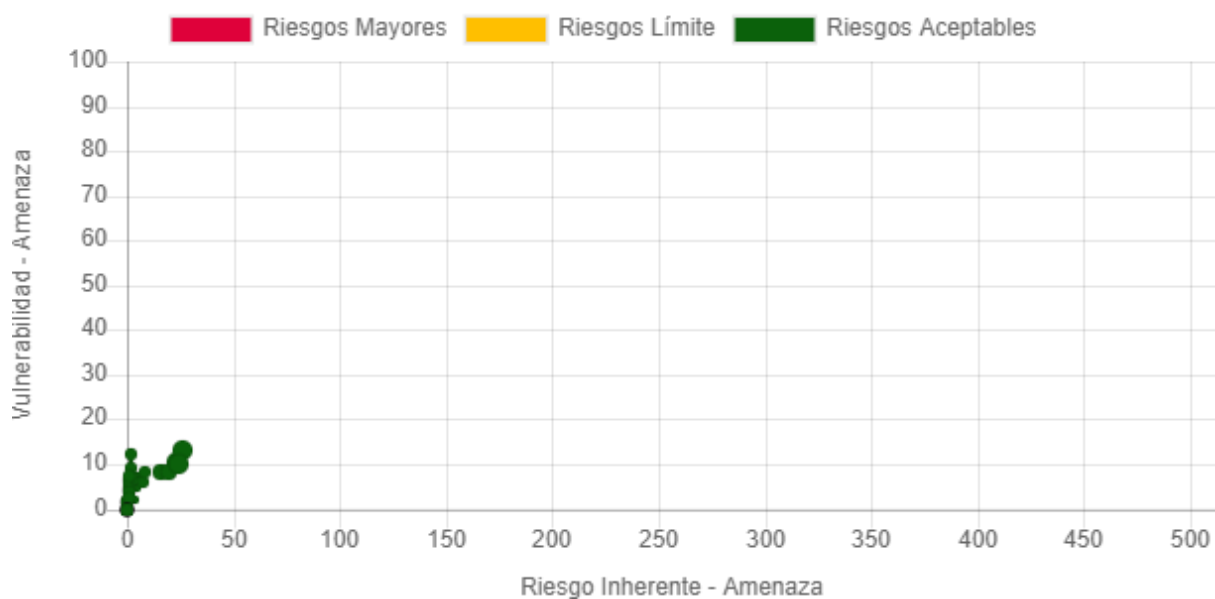
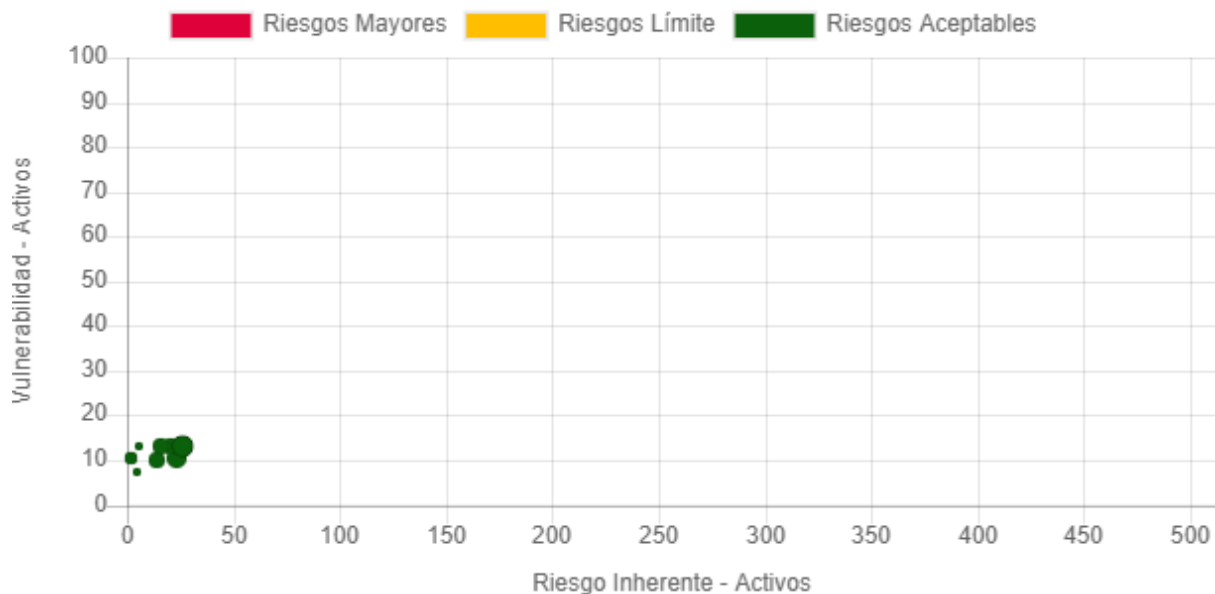


Ilustración 13

Con base en la información presentada en la gráfica 13 se puede afirmar que el riesgo total frente a amenazas es bastante bajo y no se tiene una amenaza que esté directamente expuesta a comprometer la información confidencial de la empresa. Es importante esta gráfica ya que no se tiene una amenaza susceptible a un riesgo inherente puntual, nunca se puede estar 100% seguro que no se pueda presentar alguna vulnerabilidad, pero por lo menos el indicador muestra que se tiene un correcto seguimiento y control de las posibles amenazas.

Tabla 5



El análisis se hace bastante similar cuando se revisa el riesgo inherente de una vulnerabilidad de acuerdo a los activos, y al parecer no hay ningún activo con algún riesgo puntual de ser afectado, por lo que todas las gráficas que hemos visto anteriormente dan cierto parte de tranquilidad de que se están implementando las medidas correctas y que la información de los afiliados está con altos estándares de seguridad.

6. Plan de tratamiento de riesgos

Tabla 6. Reporte de Plan de tratamiento

Responsable	Estado	Plan	Resultado
Adrián Agudelo Sánchez	Pendiente	Generar mensualmente campañas interactivas de seguridad de la información con los empleados de la empresa, con algunos simulacros realizados mediante correos fraudulentos controlados que les lleguen a los empleados con mayor riesgo de fuga de información. Capacitaciones de los riesgos legales a los que se podrían enfrentar por temas relacionados a Fraude, manipulación de información o acciones malintencionadas sobre la empresa.	Aumento de concienciación de los empleados sobre los riesgos que puede haber en las actividades del día a día sino se realizan pensando en la seguridad de la información. Cambio mentalidad de los empleados para estar un poco más prevenidos ante los eventos que suceden en el día a día
Marcos Lezcano	Pendiente	Automatizar la retirada o reasignación de derechos de acceso priorizando los aplicativos más importantes para la compañía, porque a hoy se realizan controles manuales ineficientes.	Mayor velocidad en el retiro de permisos de acceso, además de mejorar los tiempos de administración de permisos sobre los usuarios
Adrián Agudelo Sánchez	Finalizada	Definir correctamente los roles y asignaciones de las personas asignadas para la administración de permisos, de acuerdo a la especialidad de cada	Mejora en la gestión de permisos porque se tiene un encargado por aplicativo de la gestión de permisos y un

		administrador sobre aplicativos específicos de la compañía	correcto procedimiento para la implementación
Adrián Agudelo Sánchez	Pendiente	Se proponen dos acciones para tratar de disminuir el riesgo, la primera es generar auditorías periódicas para revisar los colaboradores de los proyectos de desarrollo, la otra es aprovechando que las iniciativas dentro de Protección se realizan mediante Agilismo realizar campañas para tener dentro de la ceremonia de sprint review revisión de los accesos a los códigos fuentes.	Tener menos hallazgos de usuarios con privilegios innecesarios a los códigos fuente dentro de las auditorías
Marcos Lezcano	Pendiente	Se decide crear un proceso de aprobación en un BPM (Bizagi) para garantizar que los permisos se asignen adecuadamente, garantizando la trazabilidad de la gestión	Mejorar las eficiencias de las asignaciones de permisos y lograr tener trazabilidad de las gestiones realizadas
Adrián Agudelo Sánchez	Pendiente	Se actualizará las políticas de dispositivos móviles para usar validaciones a nivel de software de las redes usadas para la conexión a aplicativos corporativos, además de continuar con la migración de todos los empleados al segundo factor de autenticación.	Disminuir el riesgo asociado a fugas de información en las aplicaciones corporativas
Marcos Lezcano	Pendiente	Se plantea revisiones periódicas del estado de los certificados digitales y la correcta custodia de las claves criptográficas mediante herramientas de almacenamiento seguro	Disminuir el riesgo asociado a fuga de información de claves criptográficas y un correcto almacenamiento
Adrián Agudelo Sánchez	Finalizada	Actualmente se tienen políticas de cara a la seguridad de la información, dónde se habla de los controles de acceso, políticas de clasificación de información, copias de seguridad y controles criptográficos y políticas de protección contra software malicioso	El resultado fue una disminución en el riesgo y un aumento de la percepción de la seguridad dentro de la compañía
Adrián Agudelo Sánchez	Pendiente	Generar políticas adecuadas para un adecuado trabajo remoto dónde se tenga correcto acceso a vpns y a los diferentes controles de ciberseguridad, adicionalmente el empleado cuente con una adecuada protección y custodia de la información	Disminuir el riesgo de fuga de información asociada al teletrabajo y una mayor adopción del mismo
Adrián Agudelo Sánchez	Pendiente	Definir correctamente a nivel de estructura de la compañía los roles específicos para administrar roles y aprobar los mismos	disminuir los riesgos asociados a aprobaciones no autorizadas o equivocadas de permisos

En esta tabla se observa en plan de tratamiento de riesgos, con su responsable, el estado en que se encuentra y la forma de mitigarlo, de la tabla anterior se puede resaltar que las políticas de la seguridad de información, control de acceso, copias de seguridad, controles criptográficos y protección contra virus ya se encuentra finalizada, con lo cual se evidencia una disminución en la afectación en el riesgo de ocurrencia de daños derivada de una buena política de protección de datos. Otras políticas que se deben tener muy en cuenta son la creación correcta de los vpn con el fin de permitir en una eventualidad el trabajo desde casa y facilitar el trabajo remoto de los empleados. A su vez se tiene que prestar atención a la creación y revocación de privilegios basándose en roles, lo cual facilita controlar el acceso a la información que tiene cada empleado.

7. Análisis de los Incidentes de Seguridad

Código	Responsable	Descripción	Causa
02862118	Marcos Lezcano	Debido a un fallo en la política de permisos un usuario que no debía poder instalar nada en su máquina pudo instalar un software sin licencia y provocó un hallazgo en una auditoría	fallo en política de permisos
02862121	Marcos Lezcano	debido a una negligencia por parte de un empleado que ingresa a su puesto de trabajo con una bebida, esta se derrama y daña computador de la empresa la cual contenía información importante de un proceso de negocio, además la información no se almacenaba en la nube	No acatamiento de políticas de control de seguridad de los activos físicos y fallo en la política de almacenamiento en la nube
02862122	Marcos Lezcano	Se encuentra dentro de un código credenciales de acceso quemadas dentro del código sin encriptación	Uso incorrecto de código fuente e incumplimiento de devsecops
02862124	Marcos Lezcano	Por negligencia del personal de seguridad se permite acceso a personal no autorizado a las instalaciones dónde se encontraba el presidente de la compañía.	fallo en control de acceso a la torre física
02862129	Marcos Lezcano	por un fallo en la seguridad del correo electrónico un correo malintencionado llegó a la bandeja de algunos usuarios, y algunos usuarios confiados lo abrieron y se inyectó un virus en sus ordenadores	Falta de concienciación de la compañía frente a correos fraudulentos
02862131	Marcos Lezcano	Claves criptográficas llegan a personal comercial que no está autorizado dado a una fuga de información desde el personal de TI	Fallo en política de control de acceso a la información y fuga de información
02862132	Marcos Lezcano	empleado de protección filtra fotos de estrategias comerciales en sus redes sociales debido a un error técnico	fallo en política de almacenamiento de información de la empresa
02862133	Marcos Lezcano	Durante el día de hoy el ambiente cloud de Azure tuvo un fallo en la disponibilidad durante una hora y no se tuvo claro con quién ponerse en contacto durante el incidente	fallo en política de contacto con proveedores
02862137	Marcos Lezcano	En una auditoría se encuentra que un usuario utilizó las credenciales de otro empleado para el ingreso a información confidencial.	fallo en política de custodia de la información
02862141	Marcos Lezcano	por error se filtró información sobre 20000 Afiliados con datos de sus rendimientos bancarios y su información personal	Fallo en política de custodia de información que implica Fuga de información sensible

En esta tabla se tuvo en cuenta los principales incidentes de seguridad que se han presentado en la compañía. teniendo en cuenta porque pudo provocarse y a su vez una pequeña descripción del impacto en la empresa. Aquí podríamos resaltar el préstamo de credenciales a un empleado de la compañía que es algo que se puede presentar fácilmente pero que puede tener hechos graves como en el caso que se planteó, donde el usuario malintencionado utiliza las credenciales para ingreso a la información confidencial, representando un fallo en la política de custodia y no divulgación de información de la empresa. Se pueden presentar Incidencias por fallos en la política de control de acceso cuándo un usuario que no debería tener permisos de administrador no tiene ningún tipo de restricciones para instalar programas o paquetes dentro de su equipo, en el caos que mencionamos se realiza una instalación de un software sin licencia y generó un hallazgo grave de auditoría por derechos de copyright. El no acatamiento de políticas de control también puede acarrear problemas a nivel de seguridad como en el ejemplo que mencionamos donde un usuario ingresa bebidas a una zona donde se encuentran equipos de cómputo y por accidente derrama líquidos ocasionando fallos en el dispositivo además aquí podría verse otro fallo si el usuario no guarda la información en la nube incumpliendo con la política de correcto custodia y almacenamiento de la información.

8. Conclusiones

- Se pudo determinar cuáles son los activos que presentan una mayor probabilidad de ocurrencia con lo cual la empresa se puede preparar para realizar una correcta mitigación en caso de presentarse el riesgo.
- La seguridad de la información debe ser uno de los pilares más importantes que debe tener en cuenta en la empresa debido a que pone en riesgo información de empleados y usuarios.
- Varias de las incidencias de seguridad presentadas en la compañía se deben a una incorrecta aplicación de las políticas de gestión de la seguridad de la información

9. Bibliografía

BIBLIOGRAFÍA

- *ISO 27002 punto por punto A10 Criptografía - Recomendaciones*. (n.d.). Retrieved April 24, 2022, from <https://normaISO27001.es/a10-criptografia/>
- *¿Qué es ISO 27000 - Seguridad de la Información? GlobalSuite Solutions*. (n.d.). Retrieved April 24, 2022, from <https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/>