DIRECTIVA INTERNA No.010
23 DE ENERO DE 2025

"Por medio de la cual se adopta el plan de tratamiento de riesgos de seguridad y privacidad de la información para la vigencia 2.025".

EL GERENTE DE LA EMPRESA DE SERVICIOS PUBLICOS DE MOCOA AGUAS MOCOA S.A E.S.P., *en ejercicio de sus facultades constitucionales, legales, en especial las conferidas en los Estatutos de Constitución de la Empresa Aguas Mocoa y*

CONSIDERANDO

Que el Articulo 15 de la Constitución Política consagra la protección de los datos personales, como el derecho fundamental que tienen todas las personas a conservar su intimidad personal y familiar, al buen nombre y a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en bancos de datos y en archivos de las entidades públicas y privadas.

Que los artículos 2.2.21.3.3 y 2.2.21.3.4 del Decreto 1083 de 2015 hacen referencia a la planeación como uno de los procesos fundamentales de la administración, considerándola como una herramienta gerencial que articula y orienta las acciones de la entidad, para el logro de los objetivos institucionales en cumplimiento de su misión particular y los fines del Estado en general; es el principal referente de la gestión, puesto que a través de ella se definen y determinan las estrategias, objetivos y metas.

Que el ejercicio de la planeación organizacional debe llevar implícitas dos características importantes: debe ser eminentemente participativo y concertado, así como tener un despliegue adecuado y suficiente en todos los niveles y espacios de la institución; por tanto, la planificación de la gestión debe asumirse como una responsabilidad corporativa, tanto en su construcción como en su ejecución y evaluación.

Que el Plan de Tratamiento de Riegos de Seguridad y Privacidad de la Información es una herramienta básica del proceso administrativo, que permitirá establecer una guía de acción clara y precisa para la administración de las Tecnologías de Información y Comunicaciones de este órgano de control, mediante la propuesta de seguridad que garantice el control de los riesgos asociados a los procesos tecnológicos existentes, en la empresa AGUAS MOCOA SA ESP, con la finalidad de salvaguardar la información y los demás activos tanto de hardware como de software.

Que el Decreto No. 612 del 4 de abril de 2018 fija las directrices para la integración de los Planes Institucionales y Estratégicos al Plan de Acción, por parte de las Entidades del Estado, entre ellos el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Que en mérito de lo expuesto

RESUELVE

ARTICULO UNO: ADOPTAR. El Plan de tratamiento de riesgos de seguridad y privacidad de la información para la Vigencia 2025, para la empresa de servicios AGUAS MOCOA S.A. E.S.P., el cual forma parte integrante de este acto administrativo.

DIRECTIVA INTERNA No.010
23 DE ENERO DE 2025

"Por medio de la cual se adopta el plan de tratamiento de riesgos de seguridad y privacidad de la información para la vigencia 2.025".

ARTICULO DOS: Divulgación. El Plan de tratamiento de riesgos de seguridad y privacidad de la información, se divulgarán a través de los medios de comunicación establecidos en la Empresa, como son publicación página web y correos electrónicos.

ARTÍCULO TRES: La presente Directiva Interna rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE

Dada en San Miguel Agreda de Mocoa, a los veintitrés (23) días del mes enero de 2025

JUAN CAMILO FAJARDO ARTEAGA
GERENTE AGUAS MOCOA S.A E.S.P.

Elaboró	Daniel Bastidas	Profesional Apoyo Gestión Tecnológica y de la información - Aguas Mocoa S.A. ESP	
Revisó	Jorge R. Bastidas	Asesor Jurídico Aguas Mocoa S.A. ESP	

EMPRESA DE SERVICIOS PUBLICOS AGUAS MOCOA S.A. E.S.P.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2.025

JUAN CAMILO FAJARDO ARTEAGA
Gerente

MOCOA PUTUMAYO

ENERO 2025

TABLA DE CONTENIDO

1. Introducción 4
2. Objetivos 5
3. Informe de análisis de riesgos Aguas Mocoa S.A. ESP 7
4. Análisis de riesgos y matriz de controles 8
5. Gestión de seguridad Aguas Mocoa S.A. ESP 10
5.1 Controles para mitigar los riesgos identificados. 10
5.2 Indicadores de gestión de seguridad de la información 11
5.2.1 Indicador Estratégico 13
5.2.2 Indicador Táctico 13
5.2.3 Indicador Operativo 14
5.3 Valoración de incidentes - Modelo de Ponemon 15
5.3.1 Software malicioso dirigido 15
5.3.2 Robo de credenciales 16
6. Análisis de amenazas y riesgos emergentes 19
6.1 Proyecciones de riesgos y amenazas de la seguridad de la información en el contexto de la empresa digital. 19
6.2 Aplicación de la ventana de AREM en AGUAS MOCOA E.S.P 20
7. SGSI Aguas Mocoa S.A. ESP 23
7.1 Diagnostico 23
7.2 Planificación 23
7.3 Operación 23
7.4 Evaluación de desempeño 24
7.5 Mejora continua 24
Conclusiones 25
Recomendaciones 28

Figuras

Figura 1. Adaptado a matriz de análisis de riesgos de Margerit en Aguas Mocoa S.A E.S.P. 8
Figura 2. Análisis de factor de riesgo..... 10
Figura 3. Ventana de AREM en Aguas Mocoa E.S.P. 20

Tablas

Tabla 1. Administración de riesgos Aguas Mocoa S.A. ESP 7
Tabla 2. Identificador GSI01. 13
Tabla 3. Identificador GSI02. 13
Tabla 4. Identificador GSI03. 14
Tabla 5. Costos totales incidentes de seguridad Modelo Ponemon – Contexto interno. 17
Tabla 6. Costos totales incidentes de seguridad Modelo Ponemon – Contexto externo. 18

1. Introducción

Este documento propone integrar la seguridad de la información en la estrategia empresarial, desarrollando políticas, implementando controles tecnológicos y capacitando al personal, en donde no solo fortalecerá la seguridad de la información, sino que también garantizará la confiabilidad de los servicios y posicionaría a la organización como un referente en seguridad de la información en el sector de servicios públicos.

Dentro del marco de gestión de riesgos, Aguas Mocoa adopta la "Guía para la administración del riesgo y del diseño de controles en entidades públicas". La metodología identifica y valora riesgos, definiendo políticas actualizadas y compartiéndolas a todos los niveles organizacionales. En el entorno empresarial actual, la seguridad de la información se vuelve crucial. Aguas Mocoa reconoce la necesidad de implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) como respuesta estratégica a las amenazas cibernéticas.

La sofisticación de ataques digitales y la complejidad del panorama cibernético plantean desafíos constantes. La introducción de una cultura digital sólida, la capacitación del personal y la implementación de controles estratégicos se revelan como medidas esenciales para contrarrestar los riesgos. Este proyecto se sumerge en la estrategia de seguridad de la información en Aguas Mocoa, trazando una ruta integral y sostenible para abordar los desafíos digitales. En un entorno digital en constante evolución, el análisis se proyecta hacia riesgos emergentes, reconociendo la necesidad de fortalecer las capacidades para salvaguardar la información ante amenazas como ransomware, malware e ingeniería social, que evolucionan constantemente. La entrada de la inteligencia artificial agrega complejidad al escenario, exigiendo una comprensión más profunda y estratégica para enfrentar los retos futuros.

2. Objetivos

Objetivo General:

- ✓ Establecer y Consolidar un Sistema Integral de Gestión de la Seguridad de la Información en Aguas Mocoa S.A. ESP, Integrando Políticas, Procesos y Controles para Garantizar la Protección de Activos de Información, Cumplir con Requisitos Legales y Regulatorios, Mitigar Riesgos Internos y Emergentes, y Fomentar una Cultura Organizacional Centrada en la Seguridad de la Información.

Objetivos Específicos:

- ✓ Definir y desarrollar una estrategia integral de seguridad de la información alineada con los objetivos estratégicos de Aguas Mocoa S.A. ESP.
- ✓ Incorporar la seguridad de la información en el Plan Estratégico de Tecnologías de la Información (PETI) de la empresa.
- ✓ Desarrollar políticas de seguridad de la información con lineamientos claros para el tratamiento de datos y activos de información.
- ✓ Instaurar controles tecnológicos y procedimientos que garanticen la confidencialidad, integridad y disponibilidad de la información.
- ✓ Proporcionar capacitación al personal sobre buenas prácticas de seguridad de la información y fomentar la conciencia sobre la importancia de la protección de datos.
- ✓ Identificar y aplicar controles adecuados, según estándares como CCN, ISO 27000 (2014) e ISO 27000 (2007), para mitigar riesgos asociados a la seguridad de la información.
- ✓ Definir métricas e indicadores operativos, tácticos y estratégicos para evaluar y mejorar continuamente la gestión de la seguridad de la información.

- ✓ Analizar la capacidad actual de Aguas Mocoa S.A. ESP para hacer frente a amenazas conocidas y latentes, mientras se investiga el impacto potencial de amenazas emergentes, especialmente las relacionadas con la inteligencia artificial, proponiendo medidas preventivas y de respuesta.

3. Informe de análisis de riesgos Aguas Mocoa S.A. ESP

En la entidad se lleva a cabo la administración de riesgos por procesos que se encuentran divididos en la estructura de la entidad, así (Ver Tabla 1.):

Tabla 1. Administración de riesgos Aguas Mocoa S.A. ESP

TIPO	PROCESOS
Estratégicos	Direccionamiento estratégico
	Ordenamiento Territorial
Misionales	Acueducto
	Alcantarillado
	Facturación y Recaudo
Apoyo	Área Administrativa
	Área talento humano
	Área financiera
	Área jurídica
	Área de almacén
Evaluación	Mejora continua
	Atención al usuario

Nota. Elaboración propia. Fuente: www.aguasmocoa.gov.co

El análisis de riesgos permite determinar las posibles causas que puedan llegar a ocasionar eventos que impacten negativamente los objetivos estratégicos de la organización al igual que el desarrollo de sus procesos, teniendo como referente el contexto interno y externo. Para lograr lo descrito, existen una serie de preguntas a las que se debe dar respuesta: ¿Qué?, ¿Cómo? y ¿Cuándo? puede suceder un hecho que afecte a la entidad y de igual forma las consecuencias que conllevaría la materialización.

Una evaluación de riesgos es un proceso que se desarrolla para medir el nivel de riesgo, cuyo objetivo es el de reducir, tratar de evitarlo, tercerizarlo o aceptarlo. Para ello se establece una matriz que permite identificar los criterios de impacto a partir de un activo y una serie de amenazas que podrían afectar dicho activo, lo que define un nivel de criticidad que permitirá establecer acciones a futuro.

4. Análisis de riesgos y matriz de controles

Se relaciona el siguiente análisis de riesgos y matriz de controles de Aguas Mocoa S.A. ESP. (CEBALLOS RUIZ , 2021), así:

Matriz_Analisis_Riesgo.xls

Nota: adaptado de la matriz para el análisis del riesgo. (Erb, 2015)

Para la valoración de riesgos se toma como referencia la matriz de análisis de riesgos de Margerit y se diligencia con base al contexto de la entidad de AGUAS MOCOA S.A. E.S.P, obteniendo los siguientes resultados (Ver Figura 3.):

Figura 1. Adaptado a matriz de análisis de riesgos de Margerit en Aguas Mocoa S.A E.S.P.

Análisis de Riesgo promedio				
		Probabilidad de Amenaza		
		Criminalidad y Político	**Sucesos de origen físico**	**Negligencia y Institucional**
Magnitud de Daño	**Datos e Información**	8,1	4,5	7,7
	Sistemas e Infraestructura	6,2	3,5	6,0
	Personal	7,2	4,0	6,9

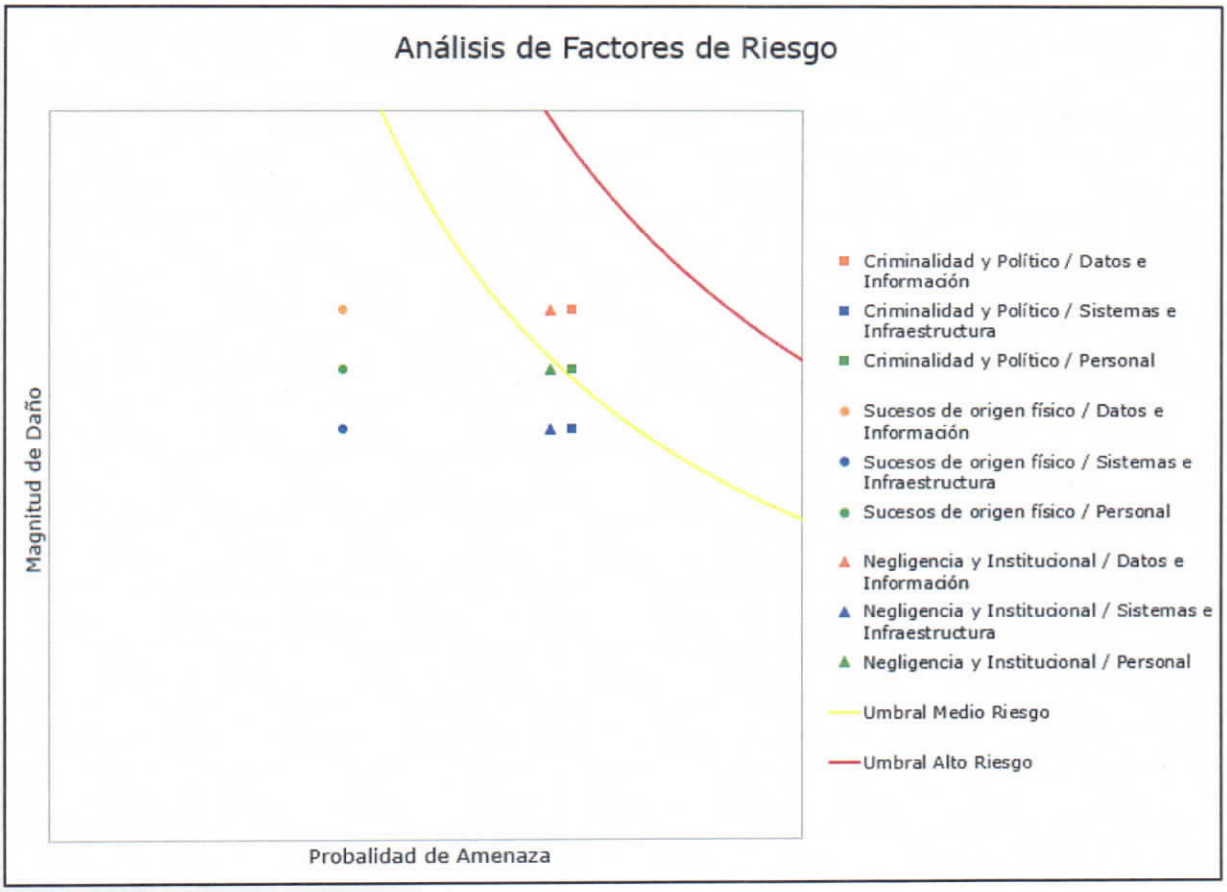
Nota. Adaptado de la matriz de análisis de riesgos de Margerit Fuente: (Aguas Mocoa S. , 2023)

Los resultados permiten evidenciar una probabilidad media en tres aspectos, el primero de ellos afecta la categoría de datos e información cuya posible amenaza se ve reflejada por la criminalidad y la política con un valor de 8.1. De este resultado se puede concluir que, al ser una institución de carácter público, podría ser susceptible de ataques por parte de actores delincuenciales cuyo objetivo sea el de obtener información relacionada con la organización que pueda comprometer el Core de esta, adicionalmente, la ausencia de políticas de seguridad digital, protección y tratamiento de datos son factores que inciden directamente en la valoración e identificación del riesgo.

Así mismo, con relación a los datos e información, la negligencia de los usuarios y las decisiones institucionales, son otro factor de consideración con un puntaje de 7.7. De esto se puede concluir que existe carencia de cultura organizacional relacionada con la protección de información y que la organización aún no ha tomado las acciones correspondientes para contrarrestar los diferentes riesgos asociados a la gestión de los usuarios con el manejo de la información o la implementación de controles que ayuden a minimizar el riesgo. Lo anterior, se evidencia en la falta de capacitación en el manejo de información confidencial y tratamiento de datos personales al personal de la empresa, lo que genera un riesgo de alta consideración.

Por último, el personal de la entidad también tiene un puntaje de 7.2 con relación a la probabilidad de amenaza de ser víctimas de actores delincuenciales por factores políticos desde el punto de vista de la organización en la que se desempeñan, siendo concurrentes los factore de riesgo que afectan a la entidad y nivel de impacto en el daño que pueden llegar a ocasionar si se materializan los riesgos, tal y como se muestra en la siguiente imagen (Ver Figura 4.).

Figura 2. Análisis de factor de riesgo.



Nota. Adaptado del análisis de factor de riesgo. Fuente: (Aguas Mocoa S. , 2023)

5. Gestión de seguridad Aguas Mocoa S.A. ESP

5.1 Controles para mitigar los riesgos identificados.

Como un primer control, en toda organización debe una buena cultura digital y para ello se requiere de capacitación constante. De acuerdo con el análisis de riesgos, la negligencia institucional tiene una valoración bastante alta por lo que se hace necesario la implementación de campañas de concientización en toda la institución, de forma que se minimice el riesgo de incidentes cuyo origen sean los usuarios finales.

En cuanto a controles orientados a contrarrestar la criminalidad, se requiere de sistemas de seguridad que minimicen la ocurrencia de incidentes de seguridad. Por una parte, para proteger los datos y la información se requieren múltiples soluciones, así:

- Seguridad de las estaciones de trabajo con soluciones antivirus endpoint con características avanzadas y acopladas a las nuevas amenazas.
- Soluciones de cifrado de información para salvaguardar los datos dentro de la red de la institución.
- Aplicar soluciones para el control de los accesos de los usuarios y la gestión de credenciales de usuario con el fin de evitar accesos no autorizados a los activos de la entidad.
- Herramientas de detección y bloqueo de amenazas a nivel de red.
- Plan de contingencia de la operación de la organización en caso de incidentes de seguridad.

Es importante tener en cuenta que la implementación de controles no evita los riesgos, solo los minimiza, con lo cual se deben estar realizando de forma periódica evaluaciones de seguridad para verificar la efectividad de los controles.

5.2 Indicadores de gestión de seguridad de la información

Teniendo en cuenta la era tecnológica de la actualidad, se observa que la cantidad de información que se procesa en las organizaciones es bastante alta. Sin embargo, el fenómeno del auge tecnológico ha conllevado el surgimiento de diferentes amenazas asociadas a la información, teniendo en cuenta que este es el activo más importante de las organizaciones. Por tal razón, es importante establecer mecanismos de protección que garanticen la salvaguarda de la confidencialidad, integridad y disponibilidad de los activos de las entidades asociados a la información y los datos.

Como instrumento para proteger la información de las organizaciones se establecieron los sistemas de gestión de seguridad de la información. En estos se establecen una serie de requisitos que las entidades deben cumplir para minimizar la posible ocurrencia de incidentes de seguridad. Adicionalmente se establecen la implementación de controles y políticas de seguridad de la información que deben ser aplicadas en todos los niveles de la organización.

Para el presente caso, se establecieron tres indicadores divididos en el nivel estratégico, táctico y operacional, con los cuales se busca mejorar la postura de seguridad de la empresa AGUAS MOCOA S.A.S, así:

El indicador estratégico busca establecer un nivel de apropiación de la cultura de seguridad digital en la organización por medio de un test que permita identificar los conocimientos básicos de seguridad de la información adquiridos por los integrantes de la organización.

El indicador táctico busca medir el nivel de aplicación de controles desplegados en los equipos de cómputo de la organización, con lo cual se busca que todos cuenten con los mínimos de seguridad deseables, que permitan contrarrestar las ciberamenazas que convergen en el ciberespacio actualmente.

El indicador operativo busca determinar la eficacia de la atención de los incidentes ocurridos al interior de la organización. Por tal razón, es importante entender que una vez gestionado un incidente que hubiese afectado la confidencialidad, integridad o disponibilidad no puede llegar a ser repetitivo puesto que indicaría que la gestión realizada no fue efectiva y eficaz.

5.2.1 Indicador Estratégico

Tabla 2. Identificador GSI01.

Identificador GSI01	
Definición	Establecer la medición del nivel de apropiación de los temas de cultura digital impartidos a los usuarios finales en todos los niveles de la organización.
Objetivo	Asegurar que los funcionarios de la entidad tengan conocimientos básicos sobre seguridad de la información, que permitan adoptar las buenas prácticas para protección de los activos de información de la entidad.
Instrumento	Test evaluativo
Fórmula	NASI= ((FAT- FNAT) /(TFE)) X100
Descripción de las variables	NASI= Nivel de apropiación de Seguridad de la Información (porcentaje) FAT= número de funcionarios que Aprueban el Test (números enteros) FNAT= número de funcionarios que No Aprueban el Test (números enteros) TFE= número Total de funcionarios de la Entidad
Responsable de la medición	Director de TI
Frecuencia de la medición	FR= trimestral
Valoración del indicador	NASI>70% Satisfactorio NASI>50% y NASI<70% Aceptable NASI<50% No Aceptable
Umbral	> 70%

Nota. Elaboración propia.

5.2.2 Indicador Táctico

Tabla 3. Identificador GSI02.

Identificador GSI02	
Definición	Verificar la aplicación de controles de seguridad a nivel de los equipos de cómputo de la entidad.
Objetivo	Garantizar que los equipos de cómputo cuenten con las herramientas de seguridad y actividades para la salvaguarda de la información definidas por la institución
Instrumento	Dominio, antivirus, actualizaciones
Fórmula	GCSI= ((EIAC- EINAC)/(TEI)) X100

Descripción de las variables	GCSI= Gestión de Controles de Seguridad de la Información (porcentaje) EIAC= Equipos Institucionales que Aplican Controles (números enteros) EINAC= Equipos Institucionales que No Aplican Controles (números enteros) TEI= número Total de Equipos Institucionales
Responsable de la medición	Director de TI
Frecuencia de la medición	FR= trimestral
Valoración del indicador	GCSI >80% Satisfactorio GCSI >50% y GCSI <70% Aceptable GCSI <50% No Aceptable
Umbral	> 80%

Nota. Elaboración propia.

5.2.3 Indicador Operativo

Tabla 4. Identificador GSI03.

Identificador GSI03	
Definición	Determinar la cantidad de incidentes ocurridos en la organización asociados a seguridad de la información donde se afecta la disponibilidad, integridad o confidencialidad de los activos de información.
Objetivo	Identificar el nivel de gestión y evolución sobre la aplicación de buenas prácticas de seguridad de la información en la entidad.
Instrumento	Reporte de incidentes
Fórmula	GIO= ((IOR)/(TIO)) X100
Descripción de las variables	GIO= Gestión de Incidentes Ocurridos (porcentaje) IOR= Incidentes Ocurridos Repetitivos (números enteros) TIO= Total de Incidentes Ocurridos (números enteros)
Responsable de la medición	Director de TI
Frecuencia de la medición	FR= trimestral
Valoración del indicador	GIO <20 % Satisfactorio GIO >20 % y GIO <30% Aceptable GIO >30 % No Aceptable
Umbral	< 20%

Nota. Elaboración propia.

5.3 Valoración de incidentes - Modelo de Ponemon

Existen múltiples amenazas que atentan contra los pilares de la seguridad de la información (confidencialidad, integridad y disponibilidad). En el caso de Aguas Mocoa S.A.S, al ser una entidad de carácter público, puede ser objetivo de ciberdelincuentes cuya motivación sea afectar la postura de seguridad en cuanto a las políticas gubernamentales en la temática a nivel país o simplemente obtener un beneficio económico.

Con relación a la valoración de incidentes, se toman dos referencias del informe de Kaspersky (2022) ajustadas al contexto local de la organización, así:

5.3.1 Software malicioso dirigido

Lo primero para tener en cuenta en este caso es la inversión en infraestructura de TI que permita la detección de este tipo de incidentes y con ello poder responder de forma inmediata ante un indicio de compromiso a los activos de la organización. Resaltando posibles conexiones maliciosas, detección de malware, indicadores de compromiso, entre otros aspectos.

En caso de presentarse la materialización de un incidente la investigación es fundamental para establecer los vectores de ataque que conllevaron a la afectación a algunos de los pilares de seguridad de la información. Detectar maquinas comprometidas y poder aislarlas para efectuar un análisis forense, requiere de personal capacitado para desempeñar esta labor y en caso de no contar con este se debe recurrir a terceros, lo que implica la contratación de servicios.

Minimizar el impacto de un incidente es primordial, puesto que, toda la infraestructura de TI se puede llegar a ver comprometida por software malicioso en caso de escalamiento lateral. Ante esto, es importante que se cuente con soluciones de seguridad enfocadas a la detección oportuna de software malicioso, teniendo en cuenta que este tipo de amenazas pueden mutar y con ello perderse el rastro dentro de la red.

Si el nivel de infección dentro de la organización llega a niveles altos, la erradicación del software malicioso puede llegar a ser una actividad compleja, llegando al punto de que sea necesario un restablecimiento total de todos los activos afectados, lo que conlleva al despliegue de todas las operaciones de soporte tanto propias como de terceros.

Finalmente, el despliegue de las lecciones aprendidas requiere de planes de acción en los que las posibles soluciones requieren de la ejecución de recursos consistentes en la adquisición de contramedidas que pueden conllevar mecanismos para el fortalecimiento de la cultura digital, hasta la implementación de herramientas de seguridad o el soporte y actualización de las existentes.

5.3.2 Robo de credenciales

Detectar credenciales robadas del entorno corporativos puede ser fundamental para prevenir la ocurrencia de incidentes de seguridad, puesto que, dependiendo del tipo de credenciales, se puede poner en riesgo la operación del negocio, llegado el caso de que dicha información permita el acceso a servicios críticos de la organización.

Posteriormente, la investigación de los hechos relacionados con fuga de credenciales requiere de análisis de los dispositivos en los que se han realizado registros, con el fin de validar el nivel de compromiso de los componentes tecnológicos de la organización.

La contención en este tipo de incidentes implica la aplicación de herramientas de autenticación o validación de credenciales desde un origen legítimo que minimice el riesgo de accesos no autorizados desde ubicaciones diferentes a las permitidas, siempre y cuando dicha actividad esté contemplada fuera de la organización.

La recuperación depende del nivel de privilegios de las credenciales robadas, puesto que si corresponden a servicios esenciales de la organización el costo de recuperación puede ser elevado, inclusive puede llevar a la pérdida total de los servicios si no se tiene respaldo de los servicios.

Las lecciones aprendidas de este tipo de incidentes se ven reflejadas en acciones orientadas al fortalecimiento de la cultura digital, para lo cual se deben realizar campañas de concientización hacia el usuario, mecanismos para fortalecer los procedimientos de autenticación, lo que conlleva a la destinación de recursos para el desarrollo de estas.

En la siguiente tabla se relacionan los costos asociados a los incidentes de seguridad de acuerdo con sus etapas:

Tabla 5. Costos totales incidentes de seguridad Modelo Ponemon – Contexto interno.

Costos totales incidentes de seguridad Modelo Ponemon – Contexto interno		
Etapa	**Costo**	**Tipo de Costo**
Detección	$50.000.000	Directo
Investigación	$10.000.000	Directo
Contención	$10.000.000	Directo
Recuperación	$50.000.000	Directo
Lecciones aprendidas	$5.000.000	Indirecto
Valor Total costo de incidentes	$125.000.000	

Nota. Adaptado del modelo Ponemon. Fuente: (Puentes P., 2021).

Por otra parte, los incidentes de seguridad pueden repercutir en la organización en el escenario externo, puesto que brinda servicios a la ciudadanía y con ello se pone en riesgo la continuidad y prestación del servicio, así:

La pérdida de información origina por medio de un ataque cibernético puede afectar el normal funcionamiento de la organización. En el caso de Aguas Mocoa S.A.S, los registros de los usuarios, los datos de pago, los registros bancarios entre otros son de gran importancia para la organización.

La interrupción de las operaciones puede impactar negativamente a la entidad, puesto que ofrece un servicio esencial a la comunidad, ante lo cual, si las actividades fueran detenidas, la afectación iría más allá del contexto interno de la empresa.

El daño de los equipos es otro aspecto a tener en cuenta, puesto que la obsolescencia tecnológica es un fenómeno recurrente en todas las organizaciones, por ende, es importante mantener soporte y garantía de los equipos en caso de daños. Así mismo en caso de fallas irreparables se debe tener un plan de contingencia tecnológica.

El valor de los ingresos dejados de recibir durante la ocurrencia de un incidente, pueden perjudicar considerablemente los estados de operación financiera de la organización, reflejado en la prestación del servicio hacia los usuarios desde el ámbito de servicio al cliente donde los pagos realizados y cuyo recaudo este orientado a la inversión en mejoras se puede ver afectado considerablemente.

Tabla 6. Costos totales incidentes de seguridad Modelo Ponemon – Contexto externo.

Costos totales incidentes de seguridad Modelo Ponemon – Contexto externo		
Etapa	Costo	Tipo de Costo
Perdida de datos	Depende del tipo de información	Indirecto
Interrupción de operaciones	Depende del tiempo de la interrupción	Directo
Daño de equipos	Depende del tipo de equipo	Directo
Pérdida de ingresos	Depende del nivel de interrupción	Indirecto
Proyección Total costo de incidentes	$200.000.000	

Nota. Adaptado del modelo Ponemon. Fuente: (Puentes P., 2021).

6. Análisis de amenazas y riesgos emergentes

6.1 Proyecciones de riesgos y amenazas de la seguridad de la información en el contexto de la empresa digital.

En el entorno digital el estado de incertidumbre es constante. Los diferentes escenarios de amenaza en lugar de disminuir siguen aumentando, ya que la innovación no es sinónimo de seguridad. El informe de (Enisa, 2023) resalta ocho grupos de amenazas dada su ocurrencia recurrente y el impacto negativo de las mismas. En este sentido las cifras de ocurrencia de incidentes informáticos irán aumentando con el paso de los años y, por ende, las organizaciones deben disponer de capacidades para hacer frente a los fenómenos que afectan la confidencialidad, disponibilidad e integridad de la información.

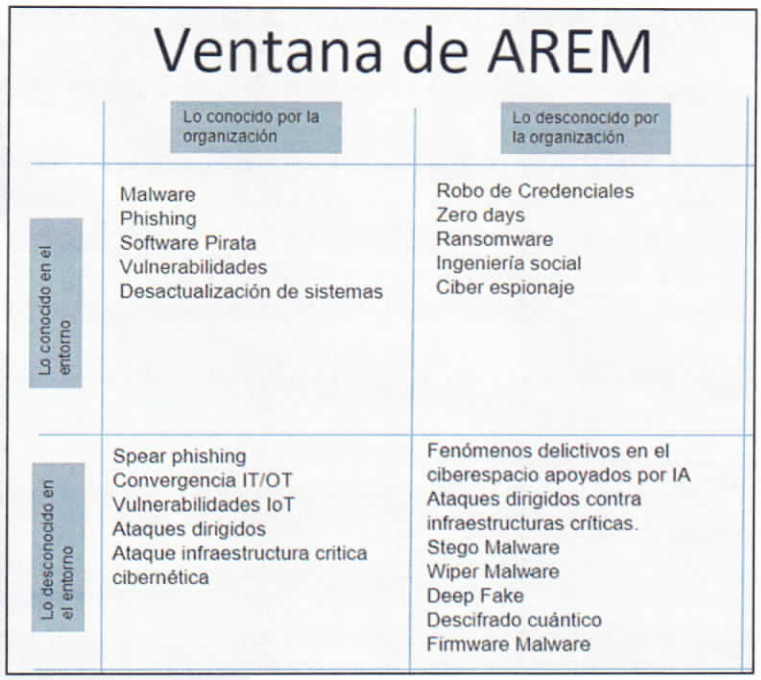
Amenazas como el ransomware y el malware, evolucionan constantemente a tal punto que un antivirus requiere de mayores recursos de cómputo para poder procesar la innumerable cantidad de componentes maliciosos que abundan e internet. Es por lo que se deben aumentar las capacidades tecnológicas de los equipos, lo que conlleva al incremento de los costos empresariales. Ante este tipo de situaciones, muchas organizaciones no cuentan con los rubros para llevar a cabo este tipo de inversiones, con lo cual, afrontan un escenario de incertidumbre con tecnologías obsoletas que no se ajustan a las nuevas necesidades del entorno interno y externo.

En este contexto, las empresas deben enfrentarse al reto de mantenerse a la vanguardia tecnológica para afrontar las nuevas amenazas persistentes, considerando que, si no, pueden desaparecer si la información, considerada el activo más valioso de las organizaciones, no se protege adecuadamente. Acciones de ingeniería social, denegaciones de servicio, manipulación de información, afectación a las cadenas de suministro, entro otras, son amenazas que se incrementarán a futuro. Bajo esta premisa, un nuevo fenómeno tecnológico ha entrado en juego y es

la inteligencia artificial que, por un lado, ha llegado para generar innovación en los procesos y automatizar aquellas tareas de carácter rutinario. Por el otro, también llega como una amenaza puesto que diferentes actores han encontrado en esta herramienta un mecanismo para mejorar e innovar el accionar delictivo en el ciberespacio, orientado a las organizaciones.

6.2 Aplicación de la ventana de AREM en AGUAS MOCOA E.S.P

Figura 3. Ventana de AREM en Aguas Mocoa E.S.P.



Nota. Adaptado de ventana de AREM (CANO MARTÍNEZ, 2023)

Teniendo en cuenta las amenazas y riesgos procesados en la ventana de AREM, se realiza el siguiente análisis de los resultados, así:

- Cuadrante amenazas y riesgos conocidos: bajo este escenario las políticas y estrategias desarrolladas en los últimos años, han llevado a que las organizaciones se preocupen por los factores de amenaza que convergen en el ciberespacio. Sin embargo, dicho conocimiento es generalizado y enfocado al despliegue y entendimiento de las altas gerencias, por lo cual,

muchas medidas de seguridad pueden estar enfocadas a fenómenos conocidos. En este orden de ideas, la entidad conoce este tipo de escenarios comunes y cuenta con algunas contramedidas para hacer frente a estas amenazas.

- Cuadrante amenazas y riesgos latentes: en este contexto, la organización se ha enterado de los diferentes ciberataques que se han realizado a nivel nacional e internacional. Esto ha conllevado a realizar análisis internos sobre cómo reaccionar y si la capacidad actual permitiría contrarrestar este tipo de amenazas, cuyo resultado ha sido un estado de incertidumbre, puesto que se requiere de recursos tanto económicos como de capacidades. Por tal motivo, se desconocen en gran medida las afectaciones de cualquiera de los escenarios planteados e inclusive si la organización actualmente hubiese sido comprometida por actores maliciosos, en el entendido que las organizaciones suelen enterarse mucho tiempo después que fueron víctimas de ciberataques.

- Cuadrante amenazas y riesgos focalizados: en el escenario de ciberataques, se han escuchado afectaciones a entidades como Keralty, EPM, entre otras. Estas cumplen de alguna forma con la prestación de servicios esenciales de la ciudadanía, situación que coincide con la actividad que cumple AGUAS MOCOA E.S.P, lo que la pone en riesgo de ciberataques dirigidos contra organizaciones que brindan servicios a la comunidad. Adicionalmente, la entidad se encuentra enmarcada en el contexto de las infraestructuras criticas lo que la hace un objetivo más valioso para los actores de amenaza, siendo posible la realización de ataques dirigidos que busquen afectar el normal funcionamiento de las operaciones, sin importar el daño causado a terceros.

- Cuadrante amenazas y riesgos emergentes: la actualización constante de tendencias en cuanto a las múltiples ciberamenazas que surgen constantemente es fundamental para las

organizaciones. En este sentido, la inteligencia artificial ha marcado un antes y un después, puesto que su creación ha servido en diversos contextos de carácter tecnológico en el ámbito de la ciberseguridad. Sin embargo, los ciberdelincuentes también han encontrado la oportunidad de mejorar las técnicas, tácticas y procedimientos haciendo uso de la IA (Inteligencia Artificial). Esto ha conllevado al surgimiento de nuevos modelamientos de amenaza que son desconocidos para muchas organizaciones, puesto que la velocidad con que estas se adecuan es menor a la evolución de las ciberamenazas, un factor que los ciberdelincuentes conocen muy bien (ISACA, 2017).

7. SGSI Aguas Mocoa S.A. ESP

Implementación de un Sistema de Gestión de Seguridad de la Información en la empresa aguas Mocoa SA ESP integrado con el Modelo de seguridad y Privacidad de la Información del MinTIC y el Modelo de Planeación y Gestión.

7.1 Diagnostico

- ✓ Nivel de madurez
- ✓ Análisis GAP

7.2 Planificación

- ✓ Contexto
- ✓ Liderazgo
  - PSPI
  - Roles y responsabilidades
- ✓ Planeación
  - Activos de información e infraestructura
  - Valoración de riesgos
  - Plan de tratamiento de riesgos de seguridad de la información.
- ✓ Soporte
  - Recursos
  - Capacitaciones
  - Comunicaciones

7.3 Operación

- ✓ Implementación de controles de seguridad de la información.
- ✓ Gestión de incidentes de seguridad de la información.

7.4 Evaluación de desempeño

- ✓ Seguimiento, medición y análisis.
- ✓ Auditoría interna.
- ✓ Revisión por la dirección.

7.5 Mejora continua

- ✓ Implementación de controles de seguridad de la información.

Conclusiones

La gestión de la seguridad de la información en Aguas Mocoa S.A. ESP emerge como una preocupación crítica que demanda acción inmediata y decidida. A pesar de contar con un Plan Estratégico de Tecnologías de la Información (PETI), la seguridad de la información no se encuentra completamente integrada en los objetivos estratégicos de la organización, lo que genera riesgos significativos para la integridad, confidencialidad y continuidad de los servicios, así como para el cumplimiento de requisitos legales y regulatorios en el sector de servicios públicos.

La comparación de políticas de seguridad con otras entidades revela un rezago en Aguas Mocoa S.A. ESP, destacando la necesidad urgente de una estrategia de seguridad integral. En este sentido, se evidencia que la falta de una estrategia de seguridad de la información pone en riesgo la confidencialidad, integridad y disponibilidad de los datos, aspectos cruciales que podrían tener consecuencias graves para la organización y sus usuarios. La importancia de contar con políticas y procedimientos sólidos en torno a la seguridad de la información se refleja claramente en las políticas de seguridad de otras entidades, como la Policía Nacional de Colombia, SETI y Construcción y Servicios (ACS), que hacen hincapié en la protección de activos de información y la gestión de riesgos.

Para abordar estas problemáticas de manera efectiva, es fundamental integrar la seguridad de la información en la estrategia de Aguas Mocoa S.A. ESP de manera coherente. Esto incluye la definición de una estrategia de seguridad alineada con los objetivos estratégicos de la empresa y la incorporación de la seguridad de la información en el PETI. Además, se deben desarrollar políticas de seguridad que proporcionen directrices claras para el tratamiento de datos y activos de información, y que definan roles y responsabilidades en la organización. La implementación de controles tecnológicos y procedimientos es esencial para garantizar la confidencialidad, integridad y disponibilidad de la

información. Asimismo, la capacitación del personal es fundamental para promover la conciencia sobre la importancia de la seguridad de la información.

La identificación de amenazas y riesgos en la organización destaca la necesidad de un enfoque preventivo, donde la educación y el compromiso del personal son fundamentales para mantener la integridad y confidencialidad de los datos, así como para asegurar la continuidad de las operaciones de la empresa. En este sentido, la aplicación de una metodología que permita la generación de acciones para la reducción de riesgos se vuelve esencial. Además, el proceso de identificación de riesgos resalta la necesidad de implementar un enfoque preventivo en la seguridad de la información, en donde la educación y compromiso del personal deben ser el factor clave para mantener la integridad y confidencialidad de los datos, así como para asegurar la continuidad de las operaciones de la empresa.

La implementación de un SGSI en Aguas Mocoa S.A. ESP no solo responde a una necesidad interna de proteger los activos de información críticos, sino que también proyecta una imagen de compromiso y responsabilidad hacia los usuarios y la comunidad en general. La inversión en cultura digital y capacitación constante refuerza el aspecto preventivo, posicionando a la organización como un ente proactivo en la gestión de riesgos digitales. Además, la aplicación de controles específicos, desde la seguridad de las estaciones de trabajo hasta las soluciones de detección y bloqueo de amenazas a nivel de red, refleja una estrategia integral para mitigar posibles vulnerabilidades.

Los indicadores estratégicos, tácticos y operativos no solo ofrecen métricas de desempeño, sino que también sirven como guías para la toma de decisiones informadas. La adaptabilidad y la mejora continua se convierten en elementos clave en este contexto, donde la ciberseguridad es una disciplina en constante evolución. La valoración de incidentes, especialmente en escenarios de software malicioso dirigido y robo de credenciales, proporciona una visión realista de los posibles

impactos y costos asociados, permitiendo una asignación eficiente de recursos para la prevención, detección y respuesta.

La proyección de costos en el ámbito interno y externo destaca la necesidad de considerar la seguridad de la información como un componente estratégico que no solo protege los intereses internos de la entidad, sino que también salvaguarda su reputación y relación con la comunidad. Aguas Mocoa S.A. ESP, mediante la implementación de este proyecto, se sitúa en una posición sólida para afrontar los desafíos digitales futuros, demostrando su compromiso no solo con la excelencia operativa, sino también con la protección integral de la información y la continuidad de sus servicios esenciales para la comunidad que sirve.

En un entorno digital caracterizado por la constante evolución de amenazas, la seguridad de la información debe ser una prioridad para las empresas. El análisis revela la necesidad de que las organizaciones comprendan y aborden no solo las amenazas conocidas, sino también aquellas emergentes, como las impulsadas por la inteligencia artificial. AGUAS MOCOA E.S.P enfrenta desafíos particulares en el contexto de ser una entidad que presta servicios esenciales, lo que la coloca en el punto de mira de posibles ciberataques. Fortalecer la infraestructura y la capacidad de respuesta se presenta como una tarea esencial para preservar la integridad operativa y la confianza del público. En este sentido, la implementación de las recomendaciones propuestas en este proyecto permitirá a la empresa no solo estar al día con las mejores prácticas de seguridad, sino también destacarse como un referente en el sector de servicios públicos en lo que respecta a la gestión de la seguridad de la información.

Recomendaciones

- ✓ Desarrollar una estrategia de seguridad de la información que se alinee con los objetivos estratégicos de Aguas Mocoa S.A. ESP, reconociendo la seguridad como un componente crítico para el éxito organizacional.
- ✓ Integrar la seguridad de la información en el Plan Estratégico de Tecnologías de la Información (PETI) de la empresa, asegurando que los aspectos de seguridad estén completamente alineados con las metas y objetivos de la organización.
- ✓ Elaborar políticas de seguridad de la información que establezcan claramente los lineamientos para el tratamiento de datos y activos de información, definiendo roles y responsabilidades dentro de la organización.
- ✓ Implementar controles tecnológicos y procedimientos que aseguren la confidencialidad, integridad y disponibilidad de la información, fortaleciendo así la seguridad de los activos digitales.
- ✓ Promover la capacitación del personal en buenas prácticas de seguridad de la información, destacando la importancia de la protección de datos y la conciencia sobre las amenazas digitales.
- ✓ Establecer un sistema de gestión de seguridad de la información que garantice la perdurabilidad de los documentos virtuales y la protección de la información sensible, asegurando su integridad a lo largo del tiempo.
- ✓ Realizar auditorías periódicas para evaluar y mejorar continuamente el sistema de seguridad de la información, identificando posibles brechas y áreas de mejora.
- ✓ Mantener actualizada la matriz de riesgos, considerando las diferentes amenazas que pueden surgir en el tiempo y ajustando las estrategias de seguridad en consecuencia.

- ✓ Capacitar al personal en gestión de riesgos, reconociendo que una mala evaluación puede conllevar a la materialización de afectaciones que impacten seriamente en los objetivos de la organización.
- ✓ Establecer políticas claras de seguridad digital y protección de datos para contrarrestar amenazas relacionadas con la criminalidad y la política.
- ✓ Implementar programas de capacitación para crear conciencia sobre la importancia de la seguridad de la información y reducir la negligencia de los usuarios, mejorando así la postura de seguridad de la organización.
- ✓ Reforzar medidas de seguridad para contrarrestar amenazas políticas, incluyendo la revisión de perfiles del personal para prevenir posibles riesgos internos.
- ✓ Desarrollar e implementar un plan integral de seguridad de la información que aborde las brechas identificadas en el análisis de riesgos, proporcionando soluciones específicas y efectivas.
- ✓ Evaluar periódicamente las métricas e indicadores establecidos para garantizar la mejora continua del sistema de gestión de seguridad de la información.
- ✓ Establecer programas de actualización tecnológica periódicos para hacer frente a las amenazas en constante evolución, especialmente aquellas impulsadas por inteligencia artificial.
- ✓ Reforzar la conciencia y capacitación en seguridad cibernética dentro de AGUAS MOCOA E.S.P para mejorar la preparación frente a amenazas conocidas y latentes.
- ✓ Implementar medidas de seguridad específicas para infraestructuras críticas, considerando la posibilidad de ciberataques dirigidos contra la entidad.
- ✓ Colaborar con entidades del sector y organismos especializados para compartir información sobre amenazas emergentes y desarrollar estrategias de defensa conjuntas.

- ✓ Establecer un plan de respuesta ante incidentes que incluya escenarios específicos relacionados con amenazas emergentes, con un enfoque particular en la inteligencia artificial.
- ✓ Asignar recursos financieros y técnicos adecuados para mantener la seguridad de la información y garantizar la continuidad de las operaciones.
- ✓ Monitorear de cerca las tendencias y desarrollos en el campo de la inteligencia artificial aplicada a la ciberseguridad para adaptarse proactivamente a nuevas amenazas, asegurando así una respuesta efectiva ante los desafíos digitales en constante evolución.

"Si crees que la tecnología puede solventar tus problemas de seguridad, entonces no entiendes los problemas y no entiendes de tecnología."

Bruce Schneier

Se firma en Mocoa, a los veintitrés (23) días del mes de enero de 2025

JUAN CAMILO FAJARDO ARTEAGA
Gerente – AGUAS MOCOA S.A. E.S.P.

Proyecto: Daniel Yesid Bastidas – Coordinador TIC
Reviso: Elías Malua Sayalpud - Jefe de Control Interno.

2. CONTROL DE CAMBIOS.

VERSIÓN N°.	FECHA DE APROBACIÓN.	DESCRIPCIÓN DEL CAMBIO.
1	23/01/2025	Se crea el plan para la vigencia 2025