Documento

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Vallecaucana de Aguas S.A. E.S.P

Contenido

1. INTRODUCCION

Hoy día, las empresas inmersas en la denominada revolución digital, reconocen el protagonismo de la información en sus procesos productivos, por tanto la importancia de tener su información adecuadamente identificada y protegida, como también la proporcionada por sus partes interesadas, enmarcada bajo las relaciones de cumplimiento, comerciales y contractuales como los son acuerdos de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia. La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio. Vallecaucana de Aguas S.A. E.S.P decide entonces vincular el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos en cumplimiento de la política de seguridad de la información aprobada por la Alta Dirección, y como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación. Los principios de protección de la información se enmarcan en:

- Confidencialidad: Propiedad que la información sea concedida únicamente a quien esté autorizado.
- Integridad: Propiedad que la información se mantenga exacta y completa.
- Disponibilidad: propiedad que la información sea accesible y utilizable en el momento que se requiera

2. OBJETIVOS GENERALES

Brindar a Vallecaucana de Aguas S.A. E.S.P una herramienta con enfoque sistemático que proporcione las pautas necesarias para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información, a través de métodos que faciliten la determinación del contexto estratégico, la identificación de riesgo y oportunidades, el análisis, la valoración y expedición de políticas, así como el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento continuo.

2.2 Objetivos Específicos

1. Validar la metodología de riesgos de Vallecaucana de Aguas S.A. E.S.P para la vigencia 2020 en lo relacionado a aquellos que puedan afectar la integridad, confidencialidad y disponibilidad de la información.
2. Identificar durante el 2020 los riesgos en los procesos de la entidad, que puedan afectar la integridad, confidencialidad y disponibilidad de la información.
3. Hacer seguimiento en el 2020 a los riesgos en los procesos del Instituto, que puedan afectar la integridad, confidencialidad y disponibilidad de la información

3. REFERENCIAS NORMATIVAS

- Ley 44 de 1993 “por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.” (Derechos de autor).
- Ley 527 de 1999 “por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.
- Ley 1273 de 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
- Decisión Andina 351 de 2015 “Régimen común sobre derecho de autor y derechos conexos”.
- CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano.
- Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.
- Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL año 2018.

4. DEFINICIONES

Definiciones Confidencialidad: Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

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

Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

Integridad: Propiedad de exactitud y completitud.

Sistema de Gestión de Seguridad de la Información: Parte del sistema de gestión general de la identidad, basada en un enfoque hacia los riesgos globales del negocio, cuyos fines son establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Política de seguridad de información: Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos de Vallecaucana de Aguas S.A. E.S.P. Se expresa en términos de probabilidad y consecuencias.

Riesgo de seguridad y privacidad: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de Contexto - Información sobre la evaluación de riesgos probabilidad y consecuencias.

5. DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La metodología de gestión de identificación, evaluación y gestión de riesgos de los sistemas de gestión vigentes de Vallecaucana de Aguas S.A. E.S.P. se basa en la Guía para la Gestión de Riesgo de Corrupción y Modelo de Gestión de Riesgos de Seguridad Digital - MGRSD. Su propósito es la identificación, estimación y evaluación de los riesgos de la entidad para definir un plan de tratamiento que se ajuste a los objetivos de cada uno de los procesos. La Gestión de Riesgos de Vallecaucana de Aguas S.A. E.S.P, incluyendo los Riesgos de Seguridad y Privacidad se lleva a cabo por los Líderes de cada proceso y lo gestionan para el cumplimiento de la misión, la visión estratégica y los objetivos misionales, con el fin de determinar el tratamiento del riesgo aceptable sobre cada uno de los riesgos identificados, teniendo en cuenta el siguiente esquema: Ciclo de la Gestión de Riesgos.

6. ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de Vallecaucana de Aguas S.A. E.S.P y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos de la compañía, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la Entidad y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Entidad. Como criterios para la gestión de riesgos de seguridad de la información se establecen:

Criterios de evaluación del riesgo de seguridad de la información:

La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso de información en Vallecaucana de Aguas S.A. E.S.P.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de Vallecaucana de Aguas S.A. E.S.P
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la Agencia.

Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la Agencia, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

Criterios de Aceptación

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos de Vallecaucana de Aguas S.A. E.S.P y de las partes interesadas

7. VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Previo a la valoración de riesgos de seguridad de la información se determina la relevancia de identificar un inventario de activos de información de los procesos, el cual será la base del enfoque de la valoración de los riesgos de seguridad de la información.

Se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para Vallecaucana de Aguas S.A. E.S.P, esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

- Análisis del riesgo o Identificación de los riesgos o Estimación del riesgo
- Evaluación del riesgo

Identificación del riesgo

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación. Los activos de información se clasifican en dos tipos:

a) Primarios:

- Procesos o subprocesos y actividades del Negocio: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.
- Información: información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.
- Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

b) De Soporte

- Hardware: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
- Software: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)
- Redes: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
- Personal: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
- Sitio: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
- Estructura organizativa: responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las amenazas que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la

valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de Vallecaucana de Aguas S.A. E.S.P. Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado

Para cada una de las amenazas analizaremos las vulnerabilidades (debilidades) que podrían ser explotadas. Finalmente se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

Estimación del riesgo

La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- Probabilidad: La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.
- Impacto: Hace referencia a las consecuencias que puede ocasionar a la Agencia la materialización del riesgo; se refiere a la magnitud de sus efectos.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

PROBABILIDAD			
Concepto	Valor	Descripción	Frecuencia
Raro	1	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años
Improbable	2	Es muy poco factible que el evento se presente.	Al menos de 1 vez en Los últimos 5 años.
Posible	3	El evento podría ocurrir en algún momento.	Al menos de 1 vez en Los últimos 2 años.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias,	Al menos de 1 vez en El último año.
Casi Certeza	5	Se espera que ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

IMPACTO		
Concepto	valor	Descripción
Insignificante	1	La materialización del riesgo puede ser controlado por los participantes del proceso, y no afecta los objetivos del proceso.
Menor	6	La materialización del riesgo ocasiona pequeñas demoras en el cumplimiento de las actividades del proceso, y no afecta significativamente el cumplimiento de los objetivos de la compañía. Tiene un impacto bajo en los procesos de otras áreas de Vallecaucana de Aguas S.A. E.S.P
Moderado	7	La materialización del riesgo demora el cumplimiento de los objetivos del proceso, y tiene un impacto moderado en los procesos de otras áreas de la compañía. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal
Mayor	11	La materialización del riesgo retrasa el cumplimiento de los objetivos de la Vallecaucana de Aguas y tiene un impacto significativo en la imagen pública de la compañía y/o de la Nación. Puede además generar impactos en: la industria; sectores económicos, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras

Catastrófico	13	La materialización del riesgo imposibilita el cumplimiento de los objetivos de Vallecaucana de Aguas S.A. E.S.P., tiene un impacto catastrófico en la imagen pública de la compañía y/o de la Nación. Puede además generar impactos en: sectores económicos, los mercados; la industria, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras

Evaluación de los riesgos

Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo, para los cuales se deberán comparar frente a los criterios básicos del contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto a la Alta Entidad.

8. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos. De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

COSTO - BENEFICIO	OPCION DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	**Evitar** el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Retener o aceptar** el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

9. MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma Entidad por tanto podrá cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte:

- Nuevos activos o modificaciones en el valor de los activos,
- Nuevas amenazas
- Cambios o aparición de nuevas vulnerabilidades

- Aumento de las consecuencias o impactos,
- Incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

(Original se encuentra firmado)

MOISES CEPEDA RESTREPO
Gerente General
VALLECAUCANA DE AGUAS S.A. E.S.P.

Elaboró y proyectó: Dr. Luis Eduardo Pineda Álzate – Director Administrativo.
Aprobó: El Firmante.

Copia. Archivo.