Código			Manual	
MSI_LAAD_v.1			Manuales de Seguridad de la Información	
Fecha de emisión				
20	11	2020		

Elaborado por:	Revisado por:	Aprobado por:
Yezid Ospina Piñeros – ETB Christian Giovanni López Hormiga - ETB	Juan Carlos Parada – Alta Consejería Distrital TIC María del Pilar Niño _ Alta Consejería Distrital TIC Lina María Cruz Silva – Empresa de Acueducto y Alcantarillado de Bogotá Sandra Patricia Palacios Jiménez – Secretaria Distrital de Planeación	Manuel Riaño – Líder Proyecto constitución de La Agencia Analítica de Datos del Distrito

TABLA DE CONTENIDO

1. Generalidades

1.1 Introducción

La principal responsabilidad de La Agencia de Analítica de Datos del Distrito, en adelante LAAD, es proteger de manera eficaz la información que gestiona, máxime cuando su gestión implica los datos de la ciudadanía del Distrito Capital. Esta protección implica prevenir la posibilidad de su uso, acceso no autorizado o fraudulento preservando su integridad y disponibilidad, mediante una adecuada gestión de riegos, la oportuna y coordinada reacción frente a la posibilidad de que estos riesgos se lleguen a materializar. De esto se trata la seguridad de la información, consigna fundamental de LAAD.

Con lo anterior y teniendo en cuenta que LAAD tiene a su cargo la integración, articulación, centralización del almacenamiento de datos y analítica de estos entre los sectores de la administración distrital, las empresas privadas y la ciudadanía, se hace necesario establecer una guía de actuación frente a la seguridad de la información.

Los manuales relacionados en este documento constituyen la manera concreta como LAAD debe asegurar la protección de la información que es gestionada con ocasión de sus funciones.

1.2 Objetivo del documento

Establecer, a partir de las Políticas de Seguridad de la Información, la guía de instrucciones para la ejecución de los aspectos básicos relacionados con la gestión de activos de información, la gestión de riesgos de seguridad de la información y la gestión de incidentes de seguridad de la información, como elementos fundamentales del qué hacer para la protección de la información gestionada por LAAD. En conjunto con las políticas de seguridad y privacidad, este documento constituye la base para la implementación de un Sistema de Gestión de Seguridad de la Información en línea con el Modelo de Seguridad y

Privacidad de la Información dispuesto por el Ministerio de Tecnologías de la Información y Comunicaciones MINTIC.

1.3 Alcance del documento

Este documento contiene los protocolos necesarios para: i. la identificación, caracterización, valoración, clasificación y seguimiento de los activos de información; ii. la identificación, análisis, valoración, tratamiento, comunicación y seguimiento de los riesgos de seguridad de la información; y, iii. la prevención, protección y detección, contención y respuesta, erradicación, recuperación y aprendizaje de los incidentes de seguridad de la información.

1.4 Glosario de términos

Activo primario de información: Es la información que es usada en LAAD para el logro de los objetivos y por tal razón, debe ser protegida.

Activo de soporte a la información: Corresponde básicamente al lugar dónde se almacenan los activos primarios de información. Tienen vulnerabilidades que son explotadas por las amenazas cuya meta es deteriorar los activos primarios.

Activos de información críticos: Son aquellos activos de información que cuentan con una criticidad MEDIA o ALTA en la matriz de identificación y clasificación de activos.

Amenaza: Origen, fuente potencial de afectación que causa un incidente no deseado y puede resultar en un daño. (Fuente: ISO 27000).

Apetito de riesgo: Es la cantidad de riesgo, de manera amplia, que LAAD está dispuesta a aceptar en la búsqueda de la generación de valor.

Capacidad de riesgo: Máxima capacidad financiera para absorber pérdidas inesperadas sin comprometer las operaciones ni las estrategias a mediano y largo plazo.

Clasificación de activos de información: Es el nivel de protección que el propietario del activo de información considera deben tener sus activos, de

acuerdo con las necesidades de seguridad requeridas desde el punto de vista del proceso de gestión bajo su cargo. El nivel de protección se basa en la confidencialidad, integridad y disponibilidad de la información

Comunicación del riesgo: Intercambio de información acerca del riesgo entre las personas o áreas responsables que toma la decisión y otras partes interesadas.

Control: Actividad de verificación, revisión, aprobación encaminada a evitar la materialización de un evento de riesgo. Está relacionado con las causas del riesgo.

Controles de seguridad de la información: Son medidas preventivas y reactivas implementadas en procesos, tecnología, infraestructura física y personas que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de los activos de información.

Mapa de calor: Es una herramienta que permite visualizar de una manera rápida el nivel de criticidad de los riesgos, facilitando su gestión.

Matriz de identificación y clasificación de activos de información: Es el instrumento mediante el cual se hace el inventario de activos de información. Allí se identifican, entre otros, sus propietarios y custodios, y se clasifican en cuanto a confidencialidad, integridad y disponibilidad con lo cual se define su criticidad.

Matriz de riesgo: Herramienta para clasificar y visualizar el riesgo, de acuerdo con su criticidad.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de probabilidad e impacto.

Probabilidad: Medida de la oportunidad de la ocurrencia, expresada como un número entre 0 y 1, donde 0 es la imposibilidad 1 es la certeza absoluta. (Fuente: ISO31000)

Riesgo: Efecto de la incertidumbre sobre los objetivos. (Fuente:ISO31000).

Riesgo inherente: Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. (Fuente:ISO31000).

Riesgo residual: Nivel resultante del riesgo después de aplicar los controles. (Fuente:ISO31000).

Tolerancia al riesgo: Monto aceptable del impacto financiero que se puede retener sin afectar la estabilidad financiera de LAAD.

Tratamiento del riesgo: Proceso de selección, diseño e implementación de medidas tendientes a modificar el riesgo y disminuir en la mayoría de los casos, su criticidad.

Vulnerabilidad: Debilidad en el sistema de información, en los procedimientos de seguridad del sistema, en los controles internos o la implementación que pudiese ser explotada o activada por una amenaza.

Contención: Evitar que el incidente siga ocasionando daños.

Evento de seguridad: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. (Fuente: ISO 27000).

Gestión de Incidentes: Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de LAAD. Minimizando su impacto en el negocio y la probabilidad que se repita.

Incidente de seguridad de la información: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información. (Fuente: ISO27035).

Recuperación: Volver el entorno afectado a su estado natural.

2 Manual de gestión de activos de información

En general la gestión de activos de información hace referencia a las actividades tendientes a identificar la información que se maneja y sus atributos, con el fin de establecer qué necesidades de protección se requieren, de manera que se pueda definir una priorización para preservar su confidencialidad, integridad y disponibilidad.

2.1 Tipos de activos de información

Lo primero que hay que reconocer es que para LAAD la información que se gestiona es un bien primordial generador de valor y es así como se entiende que es el activo principal de trabajo. En el contexto de este Manual, el término activo es todo aquello que tiene valor para LAAD, por lo que comprende cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos o funciones. Tomando como referencia el estándar ISO/IEC 27005, se distinguen dos tipos de activos de información en LAAD:

Tipo de Activo	Descripción
Primario	Actividades y procesos
	Información
De Soporte	Hardware
	Software
	Redes
	Personal
	Sitio
	Estructura organizacional

2.1.1 Activos primarios de información

Corresponde a la información, en sí misma, que es recolectada, almacenada, analizada, procesada y compartida entre los sectores de la administración distrital, las empresas privadas, la ciudadanía y al interior de LAAD. Los activos primarios de información son gestionados a través de los procesos de LAAD y por tanto en ellos recae la responsabilidad de su gestión.

2.1.2 Activos de soporte de información

Estos activos ofrecen el soporte necesario para que los activos primarios puedan ser debidamente gestionados. El estándar ISO/IEC27005 se refiere a ellos como

los activos que cuentan con vulnerabilidades, que son explotables por las amenazas cuya meta es deteriorar los activos primarios. Entre ellos se tiene: el hardware y software para almacenar activos primarios; las redes que interconectan los computadores, servidores o sistemas de información; las instalaciones físicas (dónde no solo se emplaza la tecnología sino también la documentación física) y el medio ambiente necesario para su funcionamiento (energía, aire acondicionado, agua, etc.); finalmente, podrían considerarse como activos de soporte de información a las personas quienes poseen información, conocimiento o *expertis* tal que son imprescindibles para la operación (se debe evitar la concentración de información o conocimiento).

2.2 Roles y responsabilidades

a. **Comité de seguridad y Privacidad de la Información**: Aprueba los lineamientos generales de seguridad incluyendo la gestión de activos de información y realiza seguimiento al cumplimiento de estos.

b. **Chief Information Security Officer**: Vela por el cumplimiento de los controles necesarios para cumplir con las políticas de seguridad de la información establecidas, entre ellas las relacionadas con la adecuada gestión de activos de información.

c. **Propietario de activos de información**: Persona de alto nivel de responsabilidad en LAAD, que tiene la misión de asegurar la administración correcta de los activos de información, durante todo su ciclo de vida, con el fin de proteger la información crítica de LAAD que se encuentra bajo su cargo. Vela por sus activos de información sean debidamente inventariados y autoriza los accesos a la información a su cargo.

d. **Custodio de los activos de información**: Es quien a nombre del propietario administra los controles de seguridad de la información que requieren los activos bajo su cargo.

e. **Usuario de activos de información**: Todo funcionario o contratista que requiere acceder, según sea pertinente con ocasión de sus responsabilidades, a los sistemas de información o los lugares donde se almacena y procesa información, de acuerdo con su área de trabajo

2.3 Inventarios de activos de información

2.3.1 Primarios

Los activos primarios de información deben hacer parte de un inventario cuya responsabilidad es de los propietarios de los activos de información a lo largo de los procesos dónde se gestionan tales activos. El inventario debe contener todos los datos que se presentan en los numerales del 2.4 al 2.8.

2.3.2 Soporte

Los activos de soporte de información deben ser inventariados por los custodios de los activos primarios, a través de los recursos de control operativo con lo que cuentan. Lo anterior debido a que son ellos quienes deben asegurar los controles de seguridad necesarios para proteger la información.

2.4 Identificación de activos de información

Para el inventario de activos de soporte de la información se establece el formato “Identificación y clasificación de activos de información” el cual contiene los campos descritos a continuación.

Formato de identificación y clasificación de activos de información*

Etiqueta	Proceso	Área	Propietario	Estado del activo	Nombre dl activo	Objetivo del activo	Generación del activo					Almacenamiento del activo			Uso del activo			TRD	Datos Personales			Clasificación				Criticidad	Actualizaciones
							Producción	Fuente	Estructuración	Formato	Frecuencia	Tipo	Lugar específico	Medio de almacenamiento	General	Proveedores	Legal y/o regulatorio		SI o NO	Sensibles	NNA	Confidencialidad	Integridad	Disponibilidad	Consecuencias		

** Esquema de referencia*

2.4.1 Propiedad de los activos de información

Nombre del cargo y rol del propietario del activo de información. Este rol lo tiene la misma persona que tiene el rol de dueño de proceso y es quien tiene como responsabilidades coordinar la adecuada gestión de activos de información y proteger los activos de información, determinando, entre otros, los derechos y restricciones de acceso para los usuarios específicos de sus activos. La propiedad de los activos de información puede ser compartida entre varios dueños de proceso. Es importante resaltar que aquí no se identifican nombres de personas, sino cargos.

2.5 Caracterización de los activos de información

Corresponde a los datos que permiten entender los atributos de los activos, de manera que sea posible identificar cuáles son los controles apropiados para protegerlos.

2.5.1 Generación de los activos de información

Se describen factores relacionados con quien genera o produce el activo de información. Identifica si el activo de información es producido o generado por el mismo proceso, otro proceso o, inclusive, otra entidad. También se identifica cuál es el origen de la información con la cual se construyó, produjo o generó el activo de información.

Aquí se establece si el activo de información es estructurado, es decir, si la información se encuentra o no organizada u ordenada de acuerdo con una disposición predeterminada, como, por ejemplo: cuando es un reporte obtenido de un sistema de información, es decir reportes que tengan columnas y filas estandarizadas. Se define también si el formato del activo en caso de que se trate de un archivo ofimático y la frecuencia o periodicidad con la que se genera el activo.

2.5.2 Almacenamiento de los activos de información

Corresponde al conjunto de campos que describen factores relacionados con el lugar en el que está disponible para consulta el activo de información. La ubicación del activo primario de información identifica los activos de soporte de información que serán clasificados y valorados en los inventarios de LAAD. Indica el lugar físico o electrónico en el que se almacena de manera controlada el activo de información. Es decir, el lugar oficial donde el activo permanece para su acceso y que estando fuera de allí, no se puede garantizar su exactitud y completitud.

2.5.3 Requerimientos legales y contractuales

Se identifican las leyes, decretos, resoluciones, circulares o, en general, las normas que, sólo si están debidamente identificadas en el normograma de LAAD, se constituyan en referentes del uso del activo de información.

2.5.4 Datos personales

Indica sí el activo contiene o no datos personales en los términos del régimen nacional de tratamiento de datos personales, es decir, si contiene información que permita que las personas sean identificadas o identificables, como por ejemplo datos de contacto personal, información laboral, comportamiento financiero, datos socio - económicos, información académica, gustos o tendencias, datos sensibles, etc.

Si contiene datos personales, hay que definir sí ellos son datos personales sensibles o no. Los datos personales sensibles son aquellos que puedan dar lugar a que una persona pudiera llegar a ser discriminada, siendo ejemplo de ello los siguientes: datos de salud, datos biométricos (imagen de la persona, grabación de la voz, huella digital, lectura de iris, etc.), datos de menores de edad, datos de personas en condición de vulnerabilidad o condición de

discapacidad, pertenencia a sindicatos, convicciones religiosas o filosóficas, origen racial o étnico, etc.

Igualmente es necesario identificar sí los datos personales corresponden a niños, niñas o adolescentes, teniendo en cuenta que constituyen datos sensibles y en tal sentido su tratamiento debe respetar sus derechos fundamentales y responder a su interés superior consagrado en la legislación colombiana.

2.5.5 Retención documental

Es necesario establecer si el activo de información está incluido en la Tabla de Retención Documental (TRD) de LAAD, aspecto clave para la definición del tiempo de conservación del activo de información.

2.6 Clasificación de los activos de información

Se expresan los niveles de protección que el propietario del activo de información considera deben tener sus activos, de acuerdo con las necesidades de seguridad requeridas desde el punto de vista del proceso de gestión bajo su cargo. En la siguiente ilustración se resumen los criterios de criticidad base de la definición de los niveles de protección señalados:

2.6.1 Confidencialidad

La confidencialidad, se refiere a la preservación de las restricciones o limitantes que se deben fijar para autorizar el acceso y la divulgación de los activos de información, así como los medios para la protección de la intimidad personal y propiedad de la información. Las opciones son:

Pública (Valor 1): Cualquier información no clasificada se considera como pública. La información no catalogada y por tanto pública, será aquella cuya divulgación no afecte a LAAD en términos de pérdida de imagen y/o económica.

Uso interno (Valor 2): Información que, sin ser reservada ni restringida, debe mantenerse dentro de LAAD y no debe estar disponible externamente, excepto para terceros involucrados en el tema. En el caso de terceros, deberán adquirir un compromiso contractual para no divulgar dicha información.

Restringida (Valor 3): Información sensible, interna de áreas o proyectos a los que deben tener acceso controlado otros grupos, pero no toda LAAD debido a que se puede poner en riesgo la seguridad.

Reservada (Valor 4): Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidad de negocio, potencial de fraude o requisitos legales. Los datos personales no públicos son considerados como información reservada.

2.6.2 Integridad

Se refiere a la protección contra la modificación no autorizada, exactitud o completitud de los activos de información. Los criterios de valoración aplican dependiendo de lo que causan los datos inexactos, incompletos o modificados sin autorización y la facilidad con que se superan tales consecuencias. Las opciones son:

Sin consecuencias de fácil reparación (Valor 1)

Daño moderado subsanable (Valor 2)

Daño grave difícil de reparar (Valor 3)

No reparables (Valor 4)

2.6.3 Disponibilidad

Acceso oportuno y confiable del uso de los activos de información autorizados. Las siguientes opciones se dan teniendo en cuenta que se puede estar sin el activo en funcionamiento más de un determinado tiempo al cabo del cual se comienzan a materializar riesgos financieros y operativos:

Más de 48 horas (Valor 1)

De 18 a 48 horas (Valor 2)

De 3 a 18 horas (Valor 3)

De 0 a 3 horas (Valor 4)

2.6.4 Criticidad

A partir de las valoraciones realizadas en los campos anteriores, aquí se define la criticidad del activo de información. Este campo es muy importante porque es el principal insumo para definir si al activo de información debe realizársele gestión de riesgos o no. Las opciones son:

ALTO: Activos de información en los cuales la clasificación de la información en al menos uno de los principios de seguridad (confidencialidad, integridad, y disponibilidad) es de valor 4

MEDIO: Activos de información en los cuales la clasificación de la información en al menos uno de los principios de seguridad (confidencialidad, integridad, y disponibilidad) es de valor 3, sin que ninguno sea de valor 4.

BAJO: Activos de información en los cuales la clasificación de la información en sus principios de seguridad (confidencialidad, integridad, y disponibilidad) sea máxima de valor 2.

2.7 Etiquetado de los activos de información

Además de constituirse en un número único que identifica cada activo de información entre todos los activos de información de LAAD, la etiqueta refleja la clasificación del activo en cuanto a Confidencialidad, Integridad y Disponibilidad.

La etiqueta está compuesta por:

- El código del proceso de acuerdo con la manera como se establece en el mapa de procesos de LAAD.

- Un número consecutivo dentro del proceso

- Un código de 3 números que refleja la clasificación del activo, así: CID, dónde C es confidencialidad de acuerdo con los valores de 1 a 4 establecidos en el numeral anterior, I es integridad de acuerdo con los valores de 1 a 4 establecidos en el numeral anterior y D es disponibilidad de acuerdo con los valores de 1 a 4 establecidos en el numeral anterior.

2.8 Seguimiento y actualización de los inventarios de activos de información

La revisión de este inventario, con propósitos de actualización, debe realizarse por el propietario de los activos de manera trimestral. La revisión consiste en validar si se hace necesaria una actualización. En caso de existir actualización, se identifica la fecha del seguimiento y la descripción concisa de la actualización realizada en cualquiera de los datos registrados en los campos del formato definido.

2.9 Manejo de los activos de información

Los activos de información clasificados con criticidad MEDIA y ALTA deben ser sujetos de gestión de riegos de seguridad de la información de acuerdo con las reglas establecidas en el numeral 3 del presente documento. Los activos señalados son los que se definen como activos de información críticos y por tanto

son sujetos de los controles de seguridad necesarios para preservar su confidencialidad, integridad y disponibilidad.

3 Manual de gestión de riesgos de seguridad de la información

A continuación, se definen las reglas bajo las cuales se gestionan los riesgos de seguridad de la información sobre los activos críticos de información. Estas reglas se ajustan al deber que tiene LAAD en todos sus niveles frente a la adecuada gestión de riesgos de seguridad de la información cuyo compromiso se incluye en la política integral de gestión de riesgos de LAAD.

3.1 Roles de la gestión del riesgo de seguridad de la información

Junta Directiva: Aprueba la política para la gestión integral de riesgos y conoce la tolerancia al riesgo en LAAD. Supervisa periódicamente la exposición de los riesgos de negocio de LAAD.

Gerente General: Vela por el cumplimiento efectivo de las políticas establecidas para la administración de riesgos. Apoyar el fortalecimiento del cambio cultural que implica la administración de riesgos para LAAD.

Comité de seguridad y Privacidad de la Información: Asistir al Gerente General en el cumplimiento de sus responsabilidades de supervisión en relación con la gestión de riesgos.

Gestor de riesgo y BCP: Define las estrategias de mitigación de riesgos de LAAD, las cuales deberán ser desarrolladas por los dueños de los riesgos. Realiza seguimiento a la gestión del riesgo y los planes de tratamiento a través de los indicadores para medir su eficacia y efectividad y efectúa reportes sobre el particular al comité de seguridad y privacidad de la información.

Dueños de proceso: Roles que están al frente de los procedimientos clave en LAAD y que tienen la misión de clasificar los potenciales riesgos a enfrentar respecto a la seguridad de la información y datos personales. Gestiona adecuadamente los riesgos de LAAD cumpliendo con los indicadores y

estándares establecidos. Los dueños de los procesos son los mismos propietarios de los activos de información.

3.2 Tolerancia al riesgo

Como lineamiento general para la gestión del riesgo de LAAD se definen límites de aceptación del riesgo a partir de unos criterios financieros específicos, establecidos a continuación:

Capacidad: Máxima capacidad financiera para absorber pérdidas inesperadas sin comprometer las operaciones ni las estrategias a mediano y largo plazo.

Tolerancia: Monto aceptable del impacto financiero que se puede retener sin afectar la estabilidad financiera de LAAD.

Apetito: Es la cantidad de riesgo, de manera amplia, que LAAD está dispuesta a aceptar en la búsqueda de la generación de valor. El apetito representa la actitud de LAAD hacía el riesgo actual. El apetito de riesgo define el nivel de riesgo individual transversal a LAAD que los líderes están dispuestos a tomar (o no tomar) con relación a acciones específicas, tales como adquisiciones, desarrollos, casos de uso, etc.

El valor económico del apetito de riesgo según la criticidad que éste representa para LAAD se define en 5 rangos correspondientes todos ellos a un porcentaje de la tolerancia al riesgo donde el rango 1 corresponde al 2% de la tolerancia al riesgo y el rango 5 al 10 % del mismo valor. Estos rangos constituyen los niveles de impacto que se revisan más adelante en este documento.

3.3 Análisis de contexto

Se identifican aspectos que generan impacto y pueden afectar el logro de los objetivos de LAAD. Algunos de los aspectos más importantes a revisar son:

- Lineamientos de LAAD
- Objetivos y alcance de los procesos

- Características del entorno externo (legal, reglamentario, social, político, ambiental, financiero, tecnológico y de mercado, relaciones con grupos de interés externos).
- Características del entorno interno (gobierno, estructura de LAAD, funciones y responsabilidades, políticas, objetivos, estrategias, capacidades entendidas en términos de recursos y conocimientos, relaciones con los grupos de interés internos, cultura organizacional, aspectos ambientales, de seguridad y salud en el trabajo, sistemas de información, flujos de información, procesos de toma de decisiones, normas directrices y modelos adoptados en LAAD).
- Modelo operativo de LAAD
- Alcance y objetivo de los procesos.

3.4 Identificación del riesgo

Se considera el riesgo que puede suceder, además de sus causas y consecuencias. Los riegos en LAAD se asocian a los procesos y por tanto a los activos de información que se gestionan en esos procesos.

3.4.1 Riesgo

Es importante resaltar que la gestión de riesgos operativos apunta al cumplimiento del objetivo de los procesos, no obstante, en este documento se hace referencia explícita a los riesgos de seguridad de la información en línea con la definición de riesgo de seguridad digital referido en el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD) del Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, el cual apunta a la posibilidad de que haya un uso no autorizado de la información o se afecte completitud o exactitud de esta o que los accesos autorizados no puedan ocurrir de manera oportuna.

El riesgo puede definirse como el efecto de la incertidumbre sobre los objetivos, donde:

- Un efecto es una desviación de aquello que se espera, sea positivo o negativo.
- Los objetivos tienen relación directa con la pérdida de la confidencialidad, integridad o disponibilidad de los activos críticos de información.

Al momento de darle nombre a un riesgo debe considerarse el evento que podría ocurrir sobre un activo o grupo de activos de información; este evento podría ser una actividad o elemento facilitador que frecuentemente aumenta la probabilidad o el impacto de un riesgo sobre los activos críticos de información.

3.4.2 Causa

Son acciones, situaciones o condiciones que dan origen al evento y/o permiten que el mismo se materialice. Son acontecimientos o circunstancias concretos del proceso o su ambiente, y que causan incertidumbre. No son inciertas considerando que corresponden a hechos o requisitos existentes.

Existen tres tipos de causas de riesgos de seguridad de la información:

Para confidencialidad: Acceso o uso no autorizado o fraudulento de los activos críticos de información cuya valoración en cuanto a confidencialidad sea de uso restringido o reservado.

Para integridad: Contenido incompleto y/o inexacto de los activos críticos de información cuya valoración en cuanto a integridad sea de daño grave difícil de reparar o no reparable.

Para disponibilidad: Imposibilidad de tener acceso de manera oportuna para los activos de información que requieran una disponibilidad menor a las 18 horas.

3.4.3 Consecuencia

Resultado de un evento que impacta la seguridad de los activos críticos de información del proceso que se esté analizando. Variaciones imprevistas que surgirían como consecuencia de la ocurrencia de los riesgos. Las consecuencias se encuentran directamente relacionadas con la pérdida, detrimento,

sobrecostos, reprocesos, sobrecumplimiento, entre otros. Algunos ejemplos pueden ser: pérdida de ingresos, daño a la reputación e imagen, sanciones, multas, reprocesos o sobrecostos.

3.5 Análisis y valoración del riesgo

3.5.1 Probabilidad

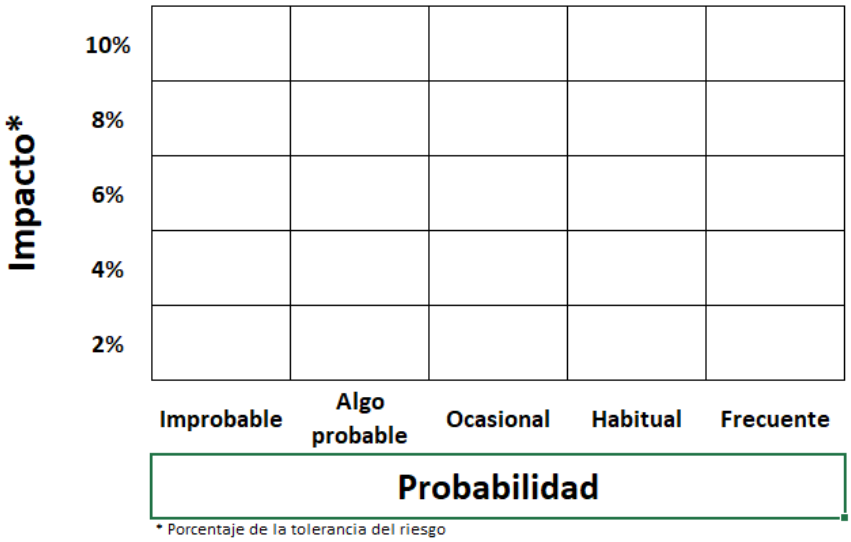
Teniendo en cuenta la información con la que se cuenta sobre el riesgo, se analiza la probabilidad de que ocurra el evento de riesgo en un periodo determinado. El resultado del análisis se debe expresar en los siguientes rangos de probabilidad, dónde 1 es el más bajo y 5 el más alto:

1. Improbable: Sólo posible en condiciones extremas
2. Algo probable: No ha ocurrido aún, pero puede llegar a suceder
3. Ocasional: Puede ocurrir y ha ocurrido de vez en cuando
4. Habitual: Ocurre con frecuencia
5. Frecuente: Ocurre casi siempre.

3.5.2 Impacto

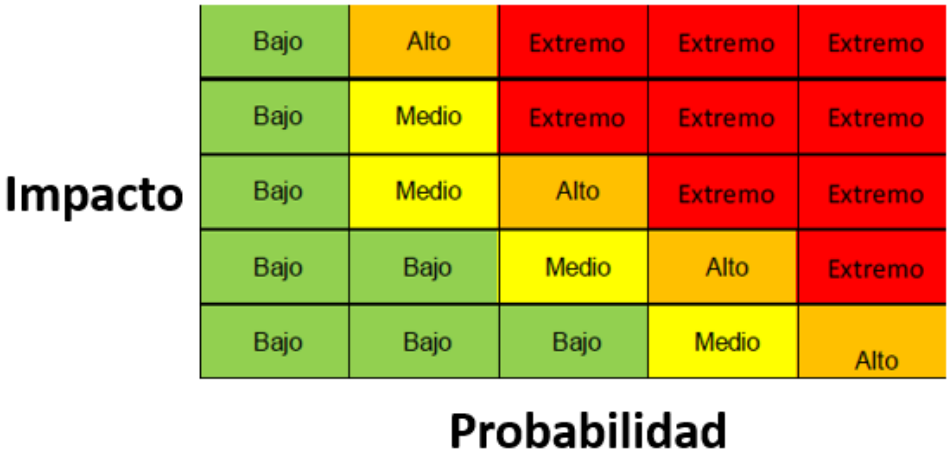
Se trata de determinar el impacto de cada riesgo si se llegara a materializar y cómo afectaría a LAAD. Con base en este concepto, se establece el nivel de impacto de cada riesgo teniendo en cuenta las pérdidas potenciales de acuerdo con las consecuencias identificadas. Es así como el impacto es un valor cuantitativo en pesos colombianos que se define teniendo en cuenta las variables establecidas en cuanto a los cinco (5) rangos establecidos en el apetito del riesgo.

Con lo anterior la relación probabilidad impacto se establece en LAAD en una matriz de 5x5, como lo muestra la siguiente ilustración:



3.5.3 Riesgo inherente

Es el riesgo que por su naturaleza no se puede separar de la situación donde se presenta, es decir, el riesgo en ausencia de medidas de control. Teniendo definidos la probabilidad y la magnitud de impacto es posible obtener una primera evaluación del riesgo, de acuerdo con el siguiente cálculo: Probabilidad X Impacto. Los resultados del nivel de riesgo inherente se distribuyen dentro del mapa de calor, determinando su criticidad:



La región verde representa la exposición al riesgo aceptable para LAAD, es decir, el primer nivel de su apetito de riesgo. Las zonas amarilla y naranja representan riesgos que podrían ser tomados, en condiciones especiales, si el costo-beneficio es representativo. Las zonas rojas, representan exposiciones al riesgo críticas para LAAD que requieren revisión, control tratamiento y monitoreo permanente.

3.5.4 Controles

Posterior al análisis y valoración del nivel de criticidad del riesgo inherente, se identifican las actividades de control implementadas actualmente sobre los riesgos, con el fin de realizar una correcta y completa evaluación de estos al momento de calificarlos (riesgo residual).

Los controles se identifican por parte del dueño del proceso para cada una de las causas de este. Es responsabilidad del dueño del proceso asegurar que estos controles se encuentren vigentes y en operación.

El proceso de Seguridad de la información cuenta con una guía denominada declaración de aplicabilidad de controles de seguridad de la información, el cual corresponde al listado de controles basado en las buenas prácticas de seguridad de la información y que se han considerado aplicables a LAAD.

La implementación de estos controles debe identificarse en los procesos para su posterior evaluación con lo que se calcula el riesgo residual.

En caso de que algunos de estos controles no estén implementados, es necesario considerar en los planes de tratamiento a que haya lugar, acciones encaminadas a su implementación.

3.5.4.1 Declaración de aplicabilidad - SOA

A continuación, la declaración de aplicabilidad (SOA, por sus siglas en inglés) de LAAD, la cual se define en el marco del estándar ISO/IEC27001 en su anexo A.

Es importante resaltar que no habrá ninguna exclusión de controles frente al señalado Anexo A:

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
1	A.5.1.1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
2	A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la SI deben ser revisadas a intervalos planificados o si ocurren cambios asegurar su adecuación y eficacia.
3	A.6.1.1	Roles y responsabilidades de la seguridad de la información	Se debe definir y asignar todas las responsabilidades de seguridad de la información
4	A.6.1.2	Segregación de tareas	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de LAAD
5	A.6.1.3	Contacto con autoridades	Se debe mantener contactos apropiados con las autoridades pertinentes

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
6	A.6.1.4	Contacto con grupos especiales de interés	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad
7	A.6.1.5	Seguridad de la Información en gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto
8	A.6.2.1	Política para los dispositivos móviles	Se debe adoptar una política y medidas de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles
9	A.6.2.2	Teletrabajo	Se debe implementar una política y medidas de soporte para proteger la información accesada, procesada o almacenada en sitios de teletrabajo.
10	A.7.1.1	Verificación de antecedentes	Debe realizarse la verificación de antecedentes para los candidatos conforme a las leyes y regulaciones relevantes, y la ética, de manera proporcional a los requisitos del negocio, la clasificación de la información a la cual tendrían acceso y los riesgos percibidos.
11	A.7.1.2	Términos y condiciones para el empleo	Los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y las de LAAD para la seguridad de la información
12	A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir que empleados y contratistas apliquen la seguridad de la información según las políticas y procedimientos de LAAD.

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
13	A.7.2.2	Toma de conciencia, educación y entrenamiento en seguridad de información	Los empleados y contratistas deben recibir acciones de toma de conciencia, educación y entrenamiento, así como actualizaciones regulares en las políticas y procedimientos según sea relevante para su función y trabajo.
14	A.7.2.3	Proceso disciplinario	Debe existir un proceso disciplinario formal y comunicado, para tomar acciones contra empleados que realicen rompimientos en la seguridad de la información.
15	A.7.3.1	Terminación o cambio en las responsabilidades del empleo	Las responsabilidades y deberes que permanezcan válidas luego de terminar el empleo o ante su cambio, deben ser definidas, comunicadas al empleado o contratista.
16	A.8.1.1	Inventario de activos	Debe identificarse la información y otros activos asociados con la información y las instalaciones de procesamiento de información, y se debe realizar y mantener un inventario de activos.
17	A.8.1.2	Propiedad de los activos	Los activos en el inventario deben tener un propietario.
18	A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y de los activos asociados con la información y las instalaciones de procesamiento de información.
19	A.8.1.4	Devolución de activos	Los empleados y usuarios de partes externas deben devolver los activos de LAAD en su posesión al terminar su empleo, contrato o acuerdo.

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
20	A.8.2.1	Clasificación de la información	La información debe clasificarse en términos de requisitos legales, valor, criticidad y sensibilidad a su divulgación o modificación no autorizada.
21	A.8.2.2	Etiquetado de la información	Deben desarrollarse e implementarse un conjunto apropiado de procedimientos para el etiquetamiento de la información según los esquemas adoptados.
22	A.8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de información adoptado.
23	A.8.3.1	Gestión de medios removibles	Deben implementarse procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por LAAD.
24	A.8.3.2	Eliminación de medios	Los medios deben eliminarse de forma segura, usando procedimientos formales, cuando ya no vayan a ser más utilizados.
25	A.8.3.3	Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
26	A.9.1.1	Política de control de acceso	Se debe establecer y documentar una política de control de acceso, la cual debe ser revisada según los requisitos del negocio y de la seguridad información

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
27	A.9.1.2	Acceso a redes y servicios de red	A los usuarios solo se les debe proveer acceso a la red y servicios de red a los cuales estén específicamente autorizados en su uso.
28	A.9.2.1	Registros y cancelación de registro de usuarios	Se debe implementar un proceso formal de registro de usuarios para permitir la asignación de derechos de usuarios
30	A.9.2.2	Suministro de acceso a usuarios	Se debe implementar un proceso formal de suministro de acceso a usuarios para asignar o revocar derechos de acceso para los tipos de usuarios a los sistemas y servicios.
30	A.9.2.3	Gestión de derechos de acceso privilegiados	Se debe restringir y controlar la asignación y uso de derechos de acceso de tipo privilegiado.
31	A.9.2.4	Gestión de información secreta de autenticación de usuarios	Se debe controlar la asignación de información secreta de autenticación a través de un proceso formal de gestión.
32	A.9.2.5	Revisión de derecho de acceso de los usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.
33	A.9.2.6	Remoción o ajuste de derechos de acceso	Se deben remover los derechos de acceso de los empleados y usuarios de partes externas a la información, así como instalaciones de procesamiento de la información, una vez terminada su vinculación, contrato o acuerdo, o ajustarse en cualquier cambio.
34	A.9.3.1	Uso de información secreta de autenticación	Se debe requerir a los usuarios el seguir las prácticas de LAAD sobre el uso de la información secreta de la información.

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
35	A.9.4.1	Restricción de acceso a la información	Se debe restringir el acceso a la información y las funciones en las aplicaciones de acuerdo con la política de control de acceso
36	A.9.4.2	Procedimientos seguros de inicio de sesión	Se debe controlar el acceso a los sistemas y aplicaciones por un procedimiento seguro de inicio de sesión, cuando esto sea requerido por la política de control de acceso
37	A.9.4.3	Gestión de contraseñas	Los sistemas de gestión de las contraseñas deben ser interactivos y asegurar contraseñas de calidad
38	A.9.4.4	Uso de programas utilitarios privilegiados	Debe estar restringido y controlado el uso de programas utilitarios que puedan ser capaces de evitar los controles del sistema y de las aplicaciones
39	A.9.4.5	Control de acceso al código fuente de las aplicaciones	Se debe restringir el acceso al código fuente de las aplicaciones
40	A.10.1.1	Política de uso de controles criptográficos	Se debe desarrollar e implementar una política para el uso de controles criptográficos para la protección información.
41	A.10.1.2	Gestión de claves	Se debe desarrollar e implementar una política para el uso, protección y gestión del ciclo de vida de las claves del cifrado.
42	A.11.1.1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad física para proteger áreas que contengan información crítica o sensible, o instalaciones de procesamiento de información.

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
43	A.11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas por controles de entrada apropiados para asegurar que solo se permite acceso al personal autorizado.
44	A.11.1.3	Aseguramiento de oficinas, áreas e instalaciones	Se debe diseñar y aplicar seguridad física para oficinas, áreas e instalaciones.
45	A.11.1.4	Protección contra amenazas externas ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
46	A.11.1.5	Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.
47	A.11.1.6	Áreas de entrega y carga	Se deben controlar, y aislar de las instalaciones de procesamiento de datos, aquellos puntos de acceso tales como áreas de entrega y de carga, así como aquellos otros puntos donde el personal no autorizado pudiese ingresar al recinto, con el fin de evitar acceso no autorizado.
48	A.11.2.1	Emplazamiento y protección de equipos	Los equipos deben estar emplazados y protegidos para reducir los riesgos de amenaza ambiental y peligros, así como la oportunidad de acceso no autorizado.
49	A.11.2.2	Servicios de soporte	Los equipos deben estar protegidos de fallas eléctricas y otras disrupciones y causadas por fallas en los servicios de soporte.
50	A.11.2.3	Seguridad del cableado	Se debe proteger de interceptación, interferencia o daño, el cableado de energía y telecomunicaciones que transporte datos o soporte de los servicios.

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
51	A.11.2.4	Mantenimiento de equipos	Los equipos deben recibir mantenimiento adecuado para garantizar disponibilidad e integridad continuadas
52	A.11.2.5	Remoción de activos	No debe retirarse equipos, información o software, de su sitio, sin autorización.
53	A.11.2.6	Seguridad de equipos y activos fuera de su sitio	Se debe aplicar seguridad a los activos fuera de su sitio de emplazamiento considerando los riesgos para los trabajos fuera de las áreas de LAAD.
54	A.11.2.7	Eliminación segura o re - uso de equipos	Los elementos de los equipos que contengan medios de almacenamiento deben ser verificados para asegurar que los datos sensibles y el software con licencia hayan sido removidos de manera segura antes de su eliminación o reúso.
55	A.11.2.8	Equipo de usuario desatendido	Los usuarios deben asegurar que los equipos desatendidos tengan protección adecuada.
56	A.11.2.9	Política de escritorio limpio	Se debe adoptar una política para escritorio limpio aplicado a documentos y medios de almacenamiento removibles, así como una política de pantalla limpia para instalaciones de procesamiento de información.
57	A.12.1.1	Procedimientos operativos documentados	Los procedimientos operativos deben estar documentados y disponibles a los usuarios que los necesiten

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
58	A.12.1.2	Gestión del cambio	Se deben controlar los cambios a LAAD, a los procesos de negocio, a las instalaciones de procesamiento de información y a los sistemas que afecten la seguridad información.
59	A.12.1.3	Gestión de la capacidad	Se debe monitorear y optimizar el uso de recursos y realizar proyecciones sobre futuros requisitos de capacidad para asegurar el desempeño requerido.
60	A.12.1.4	Separación de ambientes de prueba y de producción	Los ambientes de desarrollo, pruebas y producción deben estar separados para reducir los riesgos de acceso no autorizado o cambios al ambiente de producción.
61	A.12.2.1	Controles contra malware	Se debe implementar controles de detección, prevención y recuperación contra malware, en combinación con la toma de conciencia adecuada en los usuarios.
62	A.12.3.1	Back-up (copia de respaldo) de la información.	Se deben realizar copias de seguridad de la información del software, así como imágenes de los sistemas y ser probadas según la política de copia de respaldo.
63	A.12.4.1	Registro de eventos	Se deben producir, mantener y revisar regularmente los registros de eventos de actividad del usuario, excepciones y de seguridad información.
64	A.12.4.2	Protección de la información de registro	Las instalaciones de registro y la información de registro deben estar protegidas contra manipulación y acceso no autorizado.

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
65	A.12.4.3	Registros de administrador y del operador	Las actividades del administrador del sistema, así como del operador del sistema deben estar registrados y estos registros protegidos y revisados de manera regular.
66	A.12.4.4	Sincronización de relojes	Los relojes de los sistemas relevantes del procesamiento de información dentro de LAAD deben estar sincronizados a una única fuente de referencia de tiempo.
67	A.12.5.1	Instalación de Software en sistemas de producción	Se deben implementar procedimientos para controlar la instalación de software en sistemas operacionales.
68	A.12.6.1	Gestión de vulnerabilidades Técnicas	Se debe obtener de manera oportuna información sobre vulnerabilidades técnicas de los SI, así como de la exposición de LAAD
69	A.12.6.2	Restricciones en la instalación de software	Se deben establecer e implementar reglas para instalación de software por parte de usuarios.
70	A.12.7.1	Controles de auditoría en sistemas de información.	Los requisitos de auditoría y las actividades que incluyan verificación de sistemas de producción deben estar planeados y acordados para minimizar las disrupciones a los procesos de negocio.
71	A.13.1.1	Controles de red	Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
72	A.13.1.2	Seguridad de servicios de red	Se deben identificar e incluir en los acuerdos de servicios de red aquellos mecanismos de seguridad, niveles de servicio y requisitos de gestión de servicios red.
73	A.13.1.3	Segregación en redes	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes
74	A.13.2.1	Políticas y procedimientos para la transferencia de información	Deben estar en su lugar políticas formales, procedimientos y controles para controlar la transferencia de información mediante el uso de los tipos de instalaciones de comunicación.
75	A.13.2.2	Acuerdos de transferencia de información	Los acuerdos deben atender la transferencia segura de información del negocio entre LAAD y partes externas.
76	A.13.2.3	Mensajería electrónica	La información involucrada en mensajería electrónica debe ser protegida de manera adecuada.
77	A.13.2.4	Acuerdos de confidencialidad y no divulgación.	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad y no divulgación de la información, que reflejan las necesidades de LAAD respecto a la protección de la información.
78	A.14.1.1	Análisis y especificación de requisitos en seguridad de la información	Se deben incluir los requisitos relacionados con seguridad de la información en los requisitos de nuevos sistemas o las mejoras de los existentes.

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
79	A.14.1.2	Aseguramiento de servicios de aplicaciones en redes públicas.	Se debe proteger la información involucrada en servicios de aplicaciones que transiten por las redes públicas, frente a actividad fraudulenta, disputa en contratos, así como divulgación o autorización no autorizada.
80	A.14.1.3	Protección de transacciones en servicios de aplicaciones	La información involucrada en transacciones en servicios de aplicaciones debe estar protegida para prevenir la trasmisión incompleta, errores de enrutamiento, alteración o duplicación no autorizadas del mensaje o su reenvío.
81	A.14.2.1	Política de desarrollo seguro	Se deben establecer reglas para el desarrollo de software y sistemas para los desarrollos de LAAD
82	A.14.2.2	Procedimiento de control de cambio en sistemas	Se deben de controlar los cambios a los sistemas en el ciclo de vida de desarrollo mediante el uso de procedimientos formales de control de cambios.
83	A.14.2.3	Revisión técnica de aplicaciones luego de cambios en plataformas de producción	Cuando se realizan cambios en las plataformas de producción, las aplicaciones críticas para el negocio deben ser revisadas y probadas para asegurar que no hay impacto adverso en las operaciones o seguridad de LAAD.
84	A.14.2.4	Restricciones a cambios en los paquetes de software	Se deben rechazar las modificaciones a los paquetes de software, limitándolas a los cambios necesarios. Todo cambio debe ser controlado estrictamente

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
85	A.14.2.5	Principios de la ingeniería de sistemas seguros	Se debe establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros en esfuerzos de implementación de sistemas de información
86	A.14.2.6	Ambiente seguro de desarrollo	Las organizaciones deben establecer y proteger adecuadamente los ambientes seguros de desarrollo para el desarrollo de sistemas y esfuerzos de integración que incluyan la totalidad del ciclo de vida de desarrollo.
87	A.14.2.7	Desarrollo tercerizado	LAAD debe supervisar el desarrollo tercerizado de sistemas.
88	A.14.2.8	Prueba de seguridad de los sistemas	En el desarrollo se deben realizar pruebas de funcionalidad de la seguridad.
89	A.14.2.9	Pruebas de aceptación de sistemas.	Se deben establecer programas de pruebas de aceptación y sus criterios para sistemas de información nuevos, actualizaciones y nuevas versiones.
90	A.14.3.1	Protección de datos de pruebas	Los datos de prueba deben seleccionarse con cuidado, protegidos y controlados.
91	A.15.1.1	Política de seguridad de la información para relación con los proveedores	Se deben acordar y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos.

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
92	A.15.1.2	Incorporación de la seguridad en acuerdos con proveedores	Debe establecerse y acordarse los requisitos relevantes en seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes para infraestructura de TI.
93	A.15.1.3	Cadena de suministro para las tecnologías de la información y las comunicaciones.	Los acuerdos con proveedores deben incluir requisitos para atender los riesgos de seguridad de la información asociados con la información, los servicios de tecnologías de comunicación y la cadena de suministro de productos.
94	A.15.2.1	Seguimiento y revisión de servicios por proveedores	Las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor de manera regular.
95	A.15.2.2	Gestión de cambios en los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.
96	A.16.1.1	Responsabilidades y procedimientos	Se deben establecer responsabilidades y procedimientos para asegurar una respuesta rápida, eficaz y ordenada a incidentes de seguridad de la información.

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
97	A.16.1.2	Reportes de eventos de seguridad de la información	Los eventos de seguridad de la información deben ser reportados a través de los canales apropiados tan rápido como sea posible.
98	A.16.1.3	Reporte de debilidades en la seguridad de la información	Se debe exigir a los trabajadores y contratistas que usen los sistemas y servicios de información de LAAD que tomen nota y reporten cualquier debilidad de seguridad de la información observada o sospechada en sistemas o servicios.
99	A.16.1.4	Evaluación y decisiones en eventos de seguridad de la información	Los eventos en seguridad de la información deben ser evaluados y decidir si son clasificados como incidentes de seguridad de la información.
100	A.16.1.5	Respuesta a incidente se seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.
101	A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	El conocimiento ganado del análisis y solución de incidentes de seguridad de la información debe ser usado para reducir la probabilidad e impacto de incidentes futuros.
102	A.16.1.7	Recolección de evidencia	LAAD debe definir y aplicar procedimientos para identificar, reunir, adquirir y preservar información que pueda servir como evidencia.
103	A.17.1.1	Planeación de la continuidad de la seguridad de la información	LAAD debe determinar sus requisitos de seguridad de la información y la continuidad de la gestión de seguridad de la información en condiciones adversas, por ejemplo, una crisis o desastre.

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
104	A.17.1.2	Implementar la continuidad de la seguridad de la información	LAAD debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa.
105	A.17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de la información	LAAD debe verificar a intervalos regulares los controles establecidos e implementados de continuidad de la seguridad de la información, para asegurar que ellos permanecen válidos y son eficaces durante situaciones adversas.
106	A.17.2.1	Disponibilidad de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de información deben ser implementadas con suficiente redundancia para cumplir los requisitos de disponibilidad.
107	A.18.1.1	Identificar requisitos legales y contractuales aplicables	Todos los requisitos relevantes a nivel legislativo, estatutario, regulatorio y contractual, así como el enfoque de LAAD para cumplir con tales requisitos debe estar explícitamente identificado, documentado y actualizado para cada sistema de información y para LAAD.
108	A.18.1.2	Derechos de propiedad intelectual	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos propietarios de software.

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
109	A.18.1.3	Protección de registros	Los registros deben estar protegidos de su pérdida, destrucción, falsificación, acceso no autorizado y liberación o divulgación no autorizada de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.
110	A.18.1.4	Privacidad y protección de información identificable como personal	Se debe asegurar la privacidad y la protección de información identificable como personal según se requiera en la legislación y regulación pertinente.
111	A.18.1.5	Regulación de controles criptográficos	Los controles criptográficos deben ser usados dando cumplimiento a los acuerdos relevantes, así como a la legislación y regulaciones.
112	A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de LAAD para la gestión de la seguridad de la información y su implementación (ejemplo: objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisado de manera independiente a intervalos planeados o cuando ocurran cambios significativos.
113	A.18.2.2	Cumplimiento con políticas de seguridad y estándares	La dirección debe revisar regularmente el cumplimiento en el procesamiento de la información y sus procedimientos dentro de su área de responsabilidad, frente a las políticas de seguridad estándares y otros requisitos de seguridad.

Ítem	Controles de Seguridad de la información (ISO/IEC 27001 – Anexo A)		
	Número	**Nombre**	**Descripción**
114	A.18.2.3	Revisión de cumplimiento técnico	Los sistemas de información deben ser revisados regularmente en cuanto a su cumplimiento frente a las políticas de seguridad de la información de LAAD y estándares.

3.6 Valoración del riesgo

El objetivo es evaluar el resultado de la probabilidad e impacto dada la efectividad de los controles con los que se cuenta, de cara a definir el nivel residual del riesgo. La efectividad de los controles se establece teniendo en cuenta los siguientes aspectos:

- Si el control se encuentra implementado o no.
- Si se tiene evidencia de que el control es gestionado.
- Si el control es adecuado para la mitigación del riesgo o no.

3.6.1 Riesgo residual

Corresponde al riesgo restante después de aplicar los controles actuales, teniendo en cuanta la efectividad de esos controles. Se determina el nivel de disminución del riesgo inherente sobre el mapa de calor aplicando el porcentaje de efectividad de los controles. Lo anterior, en línea con la fórmula establecida para el cálculo de riesgo residual: Nivel de riesgo inherente * (1- Nivel de efectividad de los controles).

3.6.2 Escalamiento

A continuación, la gestión y escalamiento a realizar para a toma de decisiones frente a los diferentes niveles de riesgo:

Extremo: Gerente que corresponda

Alto: Dueño de proceso

Medio: Gestión a través de controles

Bajo: Gestión a través de controles

3.7 Tratamiento del riesgo

3.7.1 Estrategias

Se parte del nivel de criticidad de riesgo inaceptable (extremo y alto), lo cual significa que para este tipo de riesgos necesariamente se requiere de acciones adicionales a los controles actuales establecidos, las cuales deben ser diseñadas a partir de la estrategia de tratamiento. Los riesgos cuyo nivel de criticidad de riesgo sea aceptable (medio y bajo), se consideran que retienen el riesgo, pues los controles mantienen un rango aceptado por LAAD.

Las estrategias pueden ser las siguientes:

Reducir la probabilidad de ocurrencia: Medidas tendientes a prevenir la ocurrencia del riesgo o disminuir la probabilidad de ello. Las medidas actúan sobre las causas antes que el mismo se materialice.

Reducir las consecuencias: Medidas de protección que actúan después de materializado el riesgo con el propósito de evitar o limitar las consecuencias que se puedan tener.

Transferir el riesgo: Controlar las consecuencias del riesgo mediante la transferencia parcial o total de las mismas a un tercero, ya sea mediante un contrato de seguro, por subcontratación, entre otros.

Evitar el riesgo: No realizar, sustituir o eliminar la actividad que genere riesgo

Retener o aceptar el riesgo: En dado caso que no se intervenga el riesgo, se retiene. Es decir, cuando no se desarrolla ninguna acción adicional al control actual para mitigarlo. Los riesgos se pueden asumir porque se consideran que su nivel de criticidad se encuentra en los niveles de aceptación definidos actualmente por LAAD o porque razonablemente no pueden ser disminuidos, en este caso el dueño de proceso debe justificar la decisión y responsabilizarse de las consecuencias que pueden derivarse de la misma.

3.7.2 Definición de planes

En atención a la estrategia definida, se definen y documentan los planes de tratamiento o controles para mitigar los riesgos.

El dueño del proceso debe definir y acordar con las partes involucradas pertinentes el plan de tratamiento, incluyendo las actividades a desarrollar, responsables y fechas de compromiso. Los siguientes aspectos se deben tener en cuenta:

- Los responsables por ejecutar las actividades de un plan de tratamiento pueden no ser dueños de este, pero estar involucrados en su operación, por lo que deben cumplir con el compromiso establecido con el dueño de proceso.
- Dentro del plan de tratamiento de los riesgos en nivel de criticidad residual alto y extremo se deben considerar las actividades para reducir las consecuencias, es decir que se debe realizar en caso de que el riesgo se llegara a materializar.
- Una vez todas las actividades del plan de tratamiento han sido cumplidas, se debe analizar y evaluar nuevamente el riesgo correspondiente, validando su mitigación.
- En caso de que el plan de tratamiento o alguna de sus actividades se convierta en control, se debe incluir en la actualización del riesgo.

3.8 Seguimiento de riesgos

El seguimiento y la actualización del riesgo incluyen la verificación y monitoreo regular sobre el riesgo y su contexto. Este seguimiento debe realizarse por parte de los dueños de proceso y reportado al gestor de riesgos y BCP cada tres meses como mínimo o antes si se considera necesario por el dueño del proceso.

Los siguientes son los aspectos mínimos para tener en cuenta en el seguimiento:

- Revisión detallada del avance y efectividad de las actividades que componen los planes de tratamiento de riesgo
- Revisión detallada de la efectividad de los controles existentes y la necesidad de su mejora o implementación de nuevos controles.
- Detección de cambios en el contexto externo o interno, incluyendo los cambios en la identificación y evaluación del riesgo que puedan exigir revisión y ajuste del tratamiento del riesgo y su valoración.
- Identificación de la materialización del riesgo durante el periodo de seguimiento.
- Vigilancia a los riesgos de criticidad baja para determinar si continúan siendo pertinentes en ese nivel.
- Todos los riesgos activos o abiertos, independiente de su nivel de criticidad, deben monitorearse y tener registro de seguimiento(s) soportado(s) mediante evidencia objetiva y verificable.

3.9 Monitoreo de riesgos

El gestor de riesgo y BCP emitirá los informes de gestión sobre riesgos, realizando las recomendaciones y oportunidades de mejora que correspondan al Comité de Seguridad y Privacidad con el fin de desplegar la mejora en LAAD y sea debidamente ejecutada por los dueños de proceso.

3.10 Aprobación de riesgos

La aprobación de los riesgos se debe realizar por parte de cada dueño de proceso a través de un acta de aprobación de documentos. Una vez se cuenta

con la matriz de riesgos aprobada, se debe remitir información al gestor de riesgo y BCP.

4 Manual de gestión de incidentes de seguridad de la información

4.1 Modelo de gestión frente a un incidente de seguridad

Se indican una serie de actividades las cuales deben ser cumplidas con el ciclo de vida de la gestión y respuesta a un incidente de seguridad. Se define un enfoque estructurado y planificado donde LAAD indica el manejo que se le debe dar a los incidentes de seguridad de la información:

- Roles y responsabilidades dentro de LAAD
- Identificación de los eventos y gestionarlos
- Evaluación y respuesta de la manera más eficiente y adecuada
- Minimización de los impactos que se puedan presentar frente a un incidente de seguridad de la información.
- Delimitación del alcance frente a un daño o interrupción por un incidente de seguridad.
- Se establecen los riesgos que puedan ser materializados referente a los incidentes de seguridad referente a los sistemas de información.

4.1.1 Detección de Incidentes de Seguridad

En este ítem LAAD debe monitorear y verificar los componentes de control definidos para minimizar el riesgo de fuga de información, con el fin de detectar un posible incidente de seguridad de la información.

4.1.2 Atención de Incidentes de Seguridad

LAAD debe contar con procedimientos dónde se indique cómo se deben recibir y resolver los incidentes de seguridad de acuerdo con los criterios descritos en este manual.

4.1.3 Anuncios de Seguridad

LAAD debe establecer en su sistema de gestión de seguridad campañas donde se mantenga informado a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación (Web, Intranet, Correo).

4.1.4 Auditoria y trazabilidad de Seguridad Informática

LAAD debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades (contar con un cronograma con los activos críticos y su remediación).

4.1.5 Certificación de productos

Si LAAD desarrolla o implementa nuevas aplicaciones estas deben ser validadas por el grupo de seguridad desde una etapa muy temprana en el ciclo de vida de su desarrollo, las cuales se deben ajustar a los requerimientos de seguridad de la información definidos en la norma ISO27001 vigente.

4.1.6 Clasificación y priorización de servicios expuestos

Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.

4.2 Gestionar el incidente

4.2.1 Prevención

LAAD debe contar con un cronograma de actualizaciones de código (comúnmente conocidos como parches informáticos) que incluya, mínimo, a los activos que son calificados como críticos.

Toda instalación o configuración en los sistemas de información deben cambiar los usuarios y contraseñas utilizados por defecto en su instalación, estos usuarios y contraseñas deben ser custodiados por el responsable del sistema de información.

Los computadores utilizados para el manejo de información de LAAD deben contar como mínimo con un agente que detecte y elimine softwares maliciosos y deben contar con mecanismos de cifrado de información y actualización de sistemas operativos.

Los usuarios genéricos o los que se utilizan por defecto en la instalación de una solución no deben ser utilizados por los administradores de las soluciones, de ser necesario su uso, esta contraseña debe ser cambiada y documentada.

4.2.2 Recursos

LAAD debe contar con el personal idóneo para atender este tipo de incidentes, con conocimiento en normas como la ISO 27001 vigente, donde se hace referencia a los controles que se deben aplicar a los activos de información.

4.2.3 Mitigación y Remediación

LAAD debe contar con políticas de respaldo y restauración a la infraestructura categorizada como crítica.

Debe contar con registros que ayuden a proteger y donde se puedan evidenciar periódicamente las actividades de los usuarios.

Deben realizar la gestión de vulnerabilidades donde se cuente con información oportuna y se realice su respectiva gestión y remediación, disminuyendo al mínimo la materialización de algún riesgo referente a estas vulnerabilidades.

Se debe contar con mecanismos que ayuden a prevenir la fuga de información sensible para la LAAD.

4.3 Detección, evaluación, protección y análisis

4.3.1 Detección

LAAD debe contar con algún tipo de sistema que les genere alertas referentes a los sistemas de seguridad, dónde se puede identificar la caída de los componentes (servidor, base de datos, aplicación). También se debe lograr verificar qué usuario y en qué hora realiza algún tipo de actividad sobre algún sistema.

4.3.2 Evaluación y análisis

LAAD debe contar con un manual o procedimiento donde se dan los lineamientos al tratamiento de incidentes, en este se debe tener presente el impacto, urgencia y prioridad para la categorización del incidente.

4.4 Contención, erradicación, recuperación y respuesta

4.4.1 Contención

El personal encargado de la seguridad de la información debe tener presente los siguientes factores, pero no limitarlo para el tratamiento de la contención de un incidente.

LAAD debe generar lineamientos para la preservación de la evidencia y su correspondiente cadena de custodia, además de los tiempos pertinentes para cada una de las actividades o acciones que se deben tomar.

4.4.2 Erradicación

Contar con el tiempo y los recursos necesarios para tomar las acciones correspondientes en la estrategia trazada para este fin, medir el impacto en la pérdida económica y las posibles implicaciones legales que esto puede traer a LAAD. Identificar cada uno de los sistemas de información comprometidos.

4.4.3 Recuperación

Tener la copia de respaldo actualizada del sistema de información comprometida, de esta manera montarla y generar el menor impacto a LAAD y continuar con la configuración de sistemas operativos y carga manual de la información. Actualización, instalación de parches de seguridad a los sistemas comprometidos.

Código			Política	
PSI_LAAD_v.1			Manuales de Seguridad de la Información	
Fecha de emisión				
20	11	2020		

Control de Cambios:

Versión	Descripción del Cambio	Fecha del Cambio
1.0	Documento inicial	20/11/2020