TABLA DE CONTENIDO

1 INTRODUCCIÓN

Las empresas de cualquier tipo o sector se enfrentan cada vez a más riesgos procedentes de una amplia variedad de amenazas que pueden dañar de forma importante los sistemas de información y la información procesada y almacenada por ellos.

Ahora bien, debido a las situaciones derivadas de la pandemia COVID-19, se ha presentado un incremento exponencial en el acceso a la información a través de internet desde múltiples dispositivos electrónicos, el crecimiento de los servicios digitales, la utilización de medios digitales para compartir información, recuperación de datos remotos, utilización de ambientes virtuales colaborativos, entre otros, hacen que esos riesgos se incrementen.

Ante estas circunstancias y con el fin de garantizar entornos seguros, se establecen estrategias y controles adecuados que garanticen una gestión segura de los procesos del negocio dando mayor protección a la información, independientemente del medio en el que ésta se encuentre, procese, transmita, etc.

Estas estrategias y aspectos para la protección y control parten de marcos establecidos a nivel de elementos normativos que deberán ser desarrollados en las entidades del estado y de tipo asegurador y financiero para realizar una gestión y control adecuados con el fin de velar por la seguridad de la información y la gestión de la ciberseguridad.

Teniendo en cuenta lo anterior, se establece el Modelo de Seguridad y Privacidad de la Información y de Gestión de la Ciberseguridad de Previsora Seguros, cuya planificación e implementación está alineada con las necesidades y objetivos estratégicos de la compañía y a la normatividad que le aplica y se operativiza con la creación del proceso “Administrar el Sistema de Gestión de Seguridad de la Información”, en adelante SSI.

2 OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

2.1 OBJETIVO GENERAL

El objetivo general del Sistema de Gestión de Seguridad de la Información de la Compañía es preservar la integridad, confidencialidad y disponibilidad de la información de la Compañía, en cualquiera de los medios en los que se encuentre, e igualmente se pretende proteger sus activos en el ciberespacio.

2.2 OBJETIVOS ESPECÍFICOS

- Definir, reforzar y formalizar los elementos normativos sobre los temas de protección de la información.
- Establecer los mecanismos de aseguramiento físico y digital para fortalecer la confidencialidad, integridad y disponibilidad de la información de la compañía.
- Identificar y gestionar los riesgos de seguridad de la información y la ciberseguridad y mantenerlos a niveles aceptables.
- Gestionar los incidentes de seguridad de la información y Ciberseguridad y mitigar su impacto.
- Aumentar los niveles de sensibilización y cultura de los funcionarios para la protección de la información de la entidad.
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

3 ALCANCE

El Sistema de Gestión de Seguridad de la Información de la Compañía y todo el esquema normativo que de él se deriva, aplica a todos los procesos de la Compañía, sus funcionarios y todas las partes interesadas que tienen acceso a la información de la compañía.

Este documento contempla lo relacionado con seguridad de la información y ciberseguridad de la compañía. Los lineamientos relacionados con privacidad y protección de datos personales están establecidos en el MN-114 GENERAL PARA LA PROTECCIÓN DE DATOS PERSONALES y demás documentos asociados al mismo.

4 REFERENCIAS NORMATIVAS

Para el diseño, implementación, seguimiento y mejora del Sistema de Gestión de Seguridad de la Información y de Gestión de la Ciberseguridad se tendrán como referencia entre otros, los siguientes documentos:

- Resolución 500 MinTic
- CBJ – CE 052
- NTC-ISO/IEC 27001:2013 Tecnología de la información. Técnicas de seguridad.
- ISO/IEC 27002:2013 Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información.
- ISO/IEC 27032: 2012 Gestión de la Ciberseguridad.

5 GLOSARIO

- **Aceptación del riesgo**: decisión de asumir un riesgo
- **Activo:** Cualquier cosa que tenga valor para un individuo, una organización o un gobierno
- **Activo virtual:** Representación de un activo en el ciberespacio
- **Activo de Información:** Conocimiento o datos que tienen valor para la persona o la organización. Cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio.
- **Administración de Riesgos**: proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización
- **Análisis de Riesgo:** uso sistemático de a información para identificar las fuentes y estimar el riesgo
- **Aplicación:** Solución de TI, que incluye programas (software) de aplicación, datos de aplicaciones y procedimientos diseñados para ayudar a los usuarios de las organizaciones a realizar tareas específicas o manejar tipos específicos de problemas de TI, automatizando un proceso o función del negocio.
- **Ataque:** Intento de destruir, exponer, alterar, deshabilitar, robar o lograr acceso no autorizado o hacer uso no autorizado de un activo.
- **Ataque combinado:** Ataque que busca maximizar la severidad del daño y la velocidad del contagio, mediante la combinación de múltiples métodos de ataque
- **Autenticidad:** asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Avatar:** Representación de una persona que participa en el ciberespacio.
- **Bot / robot:** Programa de software automatizado utilizado para llevar a cabo tareas específicas
- **Botnet:** Software de control remoto, específicamente una colección de bots maliciosos, que se ejecutan de manera autónoma o automáticamente en computadoras comprometidas.
- **Ciberdelito (Cybercrimen):** Actividad delictiva donde servicios o aplicaciones en el ciberespacio se utilizan o son el objetivo de un crimen o donde el ciberespacio es la fuente, herramienta, blanco o el lugar de un delito.
- **Ciberespacio:** Entorno complejo que resulta de la interacción de las personas, el software y los servicios a través de internet, por medio de dispositivos tecnológicos y redes conectados al mismo, que no existe en forma física alguna.
- **Ciberintruso**: Personas u organizaciones que se registran y mantienen en direcciones URL que se asemejan a las referencias o nombres de otras organizaciones en el mundo real o en el ciberespacio.
- **Ciberprotección**: Condición de estar protegido contra consecuencias físicas, sociales, espirituales, financieras, políticas, emocionales, laborales, psicológicas, educacionales u otro tipo de consecuencias por falla, daño, error, accidente, o cualquier evento en el ciberespacio que podría ser considerado no deseable.
- **Ciberseguridad**: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio.
- **Confiabilidad de la Información:** se refiere a que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Confidencialidad:** propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Control/contramedida:** Los medios de gestión de riesgos, que incluyen las políticas, procedimientos, directrices, prácticas o estructuras organizacionales, que pueden ser de carácter administrativo, técnico, de gestión o de carácter legal.
- **Cookie <HTTP>**: Datos intercambiados entre el servidor HTTP y un navegador para almacenar la información de estado en el lado del cliente y recuperarlo después para el uso del servidor.
- **Correo electrónico no solicitado:** Correo electrónico que no es bienvenido, o no se solicitó
- **Custodio:** es una parte designada de la entidad, un cargo, proceso, o un grupo de trabajo, encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.
- **Declaración de aplicabilidad:** documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.
- **Delincuencia en Internet**: Actividad delictiva donde se utilizan los servicios o aplicaciones en Internet como objeto de un delito, o cuando la Internet es la fuente, herramienta, blanco, o el lugar de un delito
- **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Estafa (scam):** Fraude o engaño
- **Evaluación de Riesgos:** evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad que ocurran y su potencial impacto en la operatividad de la compañía.
- **Evento de seguridad de la información:** situación que indica un posible incumplimiento de la política de seguridad de la información, una falla en los controles, o una situación previamente desconocida que puede ser pertinente para la seguridad de la información.
- **Hactivismo:** Realizar piratería informática con un propósito o motivación política o social.
- **Incidente de seguridad de la información:** evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Internet**: Interconexión de redes o una colección de redes interconectadas
- **Mensaje basura (spam):** Abuso de los sistemas de mensajería electrónica para enviar indiscriminadamente mensajes masivos no solicitados
- **No repudio:** evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Parte interesada (stakeholder)** <gestión de riesgos>: Persona u organización que puede afectar, verse afectada, o percibirse a sí misma como afectada por una decisión o actividad.
- **Parte interesada (stakeholder)** <sistema>**:** Individuo u organización que tiene derecho, participación, demanda o interés en un sistema o en su posesión de características que satisfagan sus necesidades y expectativas.
- **Piratería informática (hacking):** Acceso intencional a un sistema informático sin la autorización del usuario o el propietario.
- **Potencial de ataque (attack potential):** Percepción potencial de éxito de un ataque, en caso de que un ataque sea lanzado, expresado en términos de la pericia, recursos y motivación de un atacante.
- **Principio del Mínimo Privilegio:** Todos los usuarios en cualquier momento deben contar con tan pocos privilegios como sea posible para el ingreso a un activo de información.
- **Protección en Internet (Internet safety):** Condición de estar protegido contra consecuencias físicas, sociales, espirituales, financieras, políticas, emocionales, laborales, psicológicas, educacionales u otro tipo de consecuencias por falla, daño, error, accidente o cualquier otro evento en la Internet que podría ser considerado no deseable.
- **Proveedor de servicios de aplicaciones:** Proveedor de una solución de alojamiento de software, que brinda servicios de aplicaciones que incluyen modelos entregados, a través de una página web o modelo cliente servidor.

- **Proveedor de servicios de Internet:** Organización que presta servicios de Internet a un usuario y permite a sus clientes acceder a Internet.
- **Propietario:** parte designada de la entidad, un cargo, proceso, o grupo de trabajo, que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. El término "Propietario" no implica que la persona tenga realmente los derechos de propiedad de los activos.
- **Riesgo:** Es el efecto de la incertidumbre sobre los objetivos. Los objetivos pueden abarcar diferentes aspectos (Financieros, bienestar, operativos, salud, seguridad, ambientales) y pueden aplicar a diferentes niveles en la organización (Estratégico, organizacional, procesos, proyectos, productos). El Riesgo está usualmente caracterizado por la referencia de potenciales eventos y consecuencias o la combinación de estos.
- **Seguridad de la información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.
- **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.
- **Seguridad en Internet:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información en la Internet.
- **Servicios de aplicación en el ciberespacio**: Servicios de aplicación proporcionados en el ciberespacio.
- **Servicios de aplicación:** Software con funcionalidad entregada bajo demanda a los suscriptores, a través de un modelo en línea que incluye aplicaciones basadas en web o cliente servidor.
- **Servicios de Internet:** Servicios prestados a un usuario para permitirle el acceso a Internet, a través de una dirección IP asignada, que típicamente suelen incluir servicios de autenticación, autorización y nombre de dominio.
- **Sistema de gestión de seguridad de la información – SGSI:** parte del sistema de gestión, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
- **Sistema de Información:** se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **Software de aplicación**: Software diseñado para ayudar a los usuarios a realizar tareas específicas o lidiar con tipos específicos de problemas, a diferencia del software que controla el mismo computador.
- **Software engañoso (deceptive software):** Software que realiza actividades en la computadora de un usuario sin notificarle o pedirle autorización para las acciones que el software pretende ejecutar.
- **Software espía (spyware):** Software engañoso que recopila información privada o confidencial de un usuario de computador.
- **Software malicioso**: Software diseñado con malas intenciones que contiene características o capacidades que potencialmente pueden causar daño directa o indirectamente al usuario y/o al sistema informático del usuario.
- **Software publicitario (adware):** Aplicación que, durante su funcionamiento, despliega publicidad a los usuarios o recopilan información sobre los movimientos o la conducta en línea del usuario.
- **Suplantación de identidad (phishing):** Proceso fraudulento, en una comunicación electrónica, para intentar adquirir información privada o confidencial, de manera enmascarada, haciéndose pasar por una entidad confiable.
- **Tecnología de la Información:** se refiere al hardware y software operados por la compañía o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la compañía, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

- Troyano: Software malintencionado que aparenta realizar una función deseable.
- Vector de ataque: Ruta o medio por el cual un atacante puede ganar acceso a un computador o al servidor de una red, para implementar un resultado malicioso.
- Vulnerabilidad: Debilidad de un activo o control que puede ser aprovechado por una amenaza
- Zombi computador/zombi drone: Computador que contiene software oculto que permite a la máquina ser controlada de forma remota, por lo general para llevar a cabo un ataque a otro equipo.

6 DIAGNÓSTICO

La compañía realiza anualmente un autodiagnóstico para determinar e identificar el nivel de madurez del sistema de seguridad de la información y ciberseguridad.

El autodiagnóstico se hace a través del “Instrumento de Evaluación MSPI" que es una herramienta creada por el Ministerio de Tecnologías de la Información y las Comunicaciones para establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las entidades, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente "Seguridad y Privacidad de la Información".

A partir de los resultados obtenidos del autodiagnóstico, se establecen metas, planes y actividades para mantener y mejorar en cada uno de los dominios evaluados.

7 PLANIFICACIÓN

7.1 CONTEXTO

Con base en el conocimiento del contexto de la compañía, tanto interno como externo, se definen los objetivos para la gestión de la Seguridad de la Información y del Riesgo de Ciberseguridad de la entidad, el alcance del sistema, políticas y criterios para la gestión de los riesgos.

En el análisis del contexto se identifican todas las “Partes Interesadas”, que podrían tener incidencia en los riesgos para La PREVISORA, con el fin de definir los requisitos legales, reglamentarios y las obligaciones contractuales, frente al sistema. Las partes interesadas, son responsables de la salvaguarda de los activos críticos de la compañía e igualmente son responsables de evaluar los riesgos, teniendo en cuenta las amenazas que se aplican a sus activos.

Este análisis puede ayudar en la selección de los controles para contrarrestar los riesgos y reducirlos a un nivel aceptable.

7.1.1 CONTEXTO INTERNO

Se analiza el ambiente externo o entorno que influye y/o afecta el logro de los objetivos establecidos en el plan estratégico de la organización y en consecuencia el plan de seguridad de la información.

En esta etapa se garantiza que los objetivos e intereses de las partes involucradas externas se toman en consideración al desarrollar los criterios para la gestión del riesgo de seguridad de la información y de ciberseguridad. Así mismo se definen los parámetros básicos dentro de los cuales los riesgos serán administrados y el alcance del resto del proceso de gestión de seguridad de la información y la ciberseguridad, con el fin de

entender el entorno en el que la organización opera y determinar las relaciones de la organización y su ambiente externo de negocios analizando:

- Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la compañía.
- Aspectos regulatorios o aspectos jurídicos que apliquen directa o indirectamente a la compañía, como la CBJ de la SFC y demás disposiciones que apliquen a la compañía.
- Situación financiera
- Entorno económico
- Avances tecnológicos
- Estatus político y social
- Los impulsores clave y las tendencias que tienen impacto en los objetivos de la compañía
- Las relaciones con las partes involucradas externas y sus percepciones y valores.
- Ciudadanos a los cuales la compañía brinda servicios a través del entorno digital como trámites a través de páginas web.
- Ambiente social, económico y ambiental que tengan alguna relación con las operaciones asociadas a la compañía.

En el proceso de elaborar y/o monitorear el Plan Estratégico, al analizar cada una de las interrelaciones con el entorno actual y futuro de PREVISORA, se identifican y documentan cada una de las Partes Involucradas y su rol con respecto a su efecto en el Sistema de Gestión Integral de la Compañía, incluyendo el Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

A través del monitoreo de las Partes Involucradas y su efecto en los riesgos, es que la organización y en particular la Alta Gerencia, hace la alineación y medición de manera continua el comportamiento de los riesgos en los Objetivos y Estrategias, y evalúa las implicaciones del comportamiento actual o proyectado de los riesgos, y en consecuencia modificar el plan estratégico para aprovechar las nuevas oportunidades o identificar y administrar los riesgos emergentes.

7.1.2 CONTEXTO INTERNO

Ambiente interno en el cual la Compañía busca alcanzar sus objetivos. Antes de iniciar la administración del riesgo de seguridad de la información y de ciberseguridad, es necesario conocer profundamente la organización, teniendo en cuenta los siguientes aspectos:

- Gobierno: estructura de la organización, funciones y responsabilidades
- Misión, visión, valores y cultura de la organización
- Políticas, procesos y procedimientos
- Modelo del negocio, flujos de información y procesos de toma de decisiones
- Ambiente interno de control, normas, directrices y modelos adoptados por la organización
- Capacidades en términos de recursos (humanos, capital, sistemas, procesos, etc.)

- Cultura de la organización
- Empleados, contratistas
- Sistemas de gestión de calidad, seguridad en el trabajo, seguridad de la información y gestión riesgos
- Sistemas de información o servicios.

7.1.3 PARTES INTERESADAS

Dentro del sistema de gestión integral, la compañía identifica las partes interesadas que son pertinentes al mismo, para determinar sus requisitos y obligaciones, los cuales incluyen requisitos legales y reglamentarios, así como las obligaciones contractuales, incluyendo los atinentes a seguridad y ciberseguridad.

7.2 POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La política del SGSI y Gestión de la Ciberseguridad de la Compañía, se encuentra formalizada mediante la circular CIR-320 publicada en el aplicativo de gestión documental de la compañía. En ella se definen los principios y lineamientos para la gestión de la seguridad de la información y la gestión del riesgo de ciberseguridad en la entidad y es aprobada por la Junta Directiva.

7.2.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Adicional a la política general, se establecen otra serie de políticas alineadas a los diferentes dominios y controles de las normas ISO 27001 e ISO 27002, en las que se definen los principios y lineamientos de seguridad, así como la normatividad pertinente para garantizar una adecuada gestión de la seguridad de la información en la entidad.

- Políticas normas organización y operación del SGSI
- Políticas normas de comunicaciones y operaciones
- Políticas normas para la gestión de activos de información
- Políticas de adquisición, desarrollo y mantenimiento de sistemas
- Política para la gestión de incidentes de seguridad de la información
- Políticas normas de seguridad física
- Políticas normas para la seguridad de recursos humanos
- Política para las relaciones con los proveedores
- Política de plan de continuidad de negocio
- Políticas copias de respaldo
- Políticas para uso de dispositivos móviles
- Políticas y normas para el uso de medios removibles
- Política gestión de medios de almacenamiento
- Política para uso de internet

De acuerdo con los análisis de riesgos, autodiagnóstico, resultados de auditorías etc., podrá establecer, actualizar o eliminar las políticas definidas. Adicionalmente se desarrollan procedimientos e instructivos de seguridad de la información específicos para gestionar la seguridad de la información en los diferentes procesos definidos en la entidad.

7.3 ROLES Y RESPONSABILIDADES

Mediante el documento MN – 108: MANUAL ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD se definen y documentan, de acuerdo con la política de seguridad de la información, las responsabilidades y roles de las personas que forman parte del sistema de seguridad de la información y ciberseguridad de la compañía.

7.4 ACTIVOS DE INFORMACIÓN

La compañía define y aplica un proceso para la identificación y clasificación de la información que permite:

- Identificar qué activos de información van a hacer parte del Inventario, que aportan valor agregado al proceso y por tanto necesitan ser protegidos de potenciales riesgos.
- Clasificar los activos de acuerdo con los tres principios de seguridad de la información: integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados.

Así mismo se establece la responsabilidad de actualizar el inventario y la clasificación de los activos por los líderes de los procesos al menos una vez al año o cada vez que exista un cambio en el proceso.

Este proceso se encuentra formalización en los siguientes documentos:

- CIRCULAR - 379 POLÍTICAS NORMAS PARA LA GESTIÓN DE ACTIVOS DE INFORMACIÓN: Define un proceso repetible, sistémico y orientado a gestionar los activos de información de la Compañía donde cada uno de los procesos identifiquen y clasifiquen sus activos.

- IN-SSI-001 GESTIÓN DE ACTIVOS DE LA INFORMACIÓN EN LA PREVISORA S.A: Establece los criterios, condiciones y actividades a desarrollar para la identificación, clasificación y gestión de los activos de información de Previsora S.A.

Como resultado de la aplicación del proceso se tiene el documento AI-007 que contiene el consolidado de las matrices de activos de información de todos los procesos de la compañía.

7.5 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La compañía define y aplica un proceso de valoración de riesgos de la seguridad de la información sobre los activos de información críticos, que permite:

- Identificar los riesgos que causen la perdida de confidencialidad, integridad y disponibilidad de la información, así como la continuidad de la operación de la entidad dentro del alcance del sistema.
- Definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia.
- Determinar los niveles de riesgo.
- Priorizar los riesgos analizados para su tratamiento.

Esta metodología fue aprobada por la Junta Directiva de la compañía y se encuentra documentada en el MN-188 MANUAL DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

7.6 PLAN DE TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La compañía mediante la metodología para la gestión de riesgos de seguridad de la información define los niveles de aceptables de riesgo.

Para aquellos riesgos que no estén dentro de los niveles aceptables, se aplicar un proceso de tratamiento de riesgos de la seguridad de la información, para permitir la identificación de controles pertinentes y apropiados para el tratamiento de riesgos.

7.6.1 DECLARACIÓN DE APLICABILIDAD (SOA)

La compañía elabora la Declaración de Aplicabilidad o Statement of Applicability (SOA), que es el documento que lista los objetivos y controles que se van a implementar en la Compañía, así como las justificaciones de aquellos controles que no van a ser implementados.

El documento es generado o actualizado posterior a la identificación de riesgos, definición de controles, identificación de requisitos legales, regulatorios y contractuales, así como de revisar las necesidades de la compañía.

7.7 RECURSOS

La compañía determina y proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información, lo cual se evidencia en el presupuesto anual asignado en los rubros de seguridad informática y demás rubros asignados a las diferentes áreas para la implementación o ejecución de controles que apoyen la seguridad de la información.

7.8 COMPETENCIA, TOMA DE CONCIENCIA Y CAPACITACIÓN

Con el fin de garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad de la información y la ciberseguridad, a todos los funcionarios de la compañía, se desarrollan las siguientes actividades anualmente:

- Curso virtual de seguridad de la información y ciberseguridad para nuevos funcionarios (requisito en el proceso de vinculación)
- Charla de sensibilización en el proceso de inducción de nuevos funcionarios.
- Curso virtual de reinducción obligatorio para todos los funcionarios de la compañía (hace parte del plan de formación de la organización)
- Remisión de mensajes de sensibilización a todos los usuarios, a través de los buzones de comunicación corporativo.
- Campañas de comunicación por demanda (según requerimiento)
- Otras actividades como webinars, charlas o pruebas de ingeniería social

8 EVALUACIÓN Y DESEMPEÑO

8.1 INDICADORES

La compañía establece indicadores para evaluar el desempeño y eficacia del SGSI. Las hojas de vida de los indicadores se encuentran publicados en la caracterización del proceso y la medición queda registrada en la herramienta que la compañía designe para tal fin.

8.2 AUDITORÍA INTERNA

La oficina de control interno de la entidad es la encargada de efectuar auditorías internas para verificar el estado del sistema de seguridad de la información, de acuerdo con el plan anual de auditorías aprobado por la alta dirección.

8.3 REVISIÓN POR LA DIRECCIÓN

Semestralmente se presenta al comité de seguridad de la información y a la Junta Directiva de la entidad, un informe de la gestión desarrollada respecto a la seguridad de la información y ciberseguridad de la compañía.

Adicionalmente se establecen revisiones anuales por parte del comité de seguridad de la información (comité de presidencia), para determinar la conveniencia, adecuación y eficacia del sistema de gestión de seguridad.

9 MEJORAMIENTO CONTÍNUO

De acuerdo con los resultados obtenidos de la fase de evaluación de desempeño se determinan e implementan las acciones oportunas para mitigar las debilidades identificadas los cuales son tratadas de acuerdo con el Proceso de Mejora Continua y son documentadas en los planes de mejoramiento de la compañía.

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE (S)	Sandra Cediel B	Sandra Cediel B	María Margarita González
CARGO (S)	Especialista Gerencia de Riesgos	Especialista Gerencia de Riesgos	Gerente de Riesgos

CONTROL DE CAMBIOS	
VERSIÓN	CAMBIO REALIZADO
1	Se crea el documento