POLITICAS DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD

SGSIC ISO 27001:2022

1 DE AGOSTO DE 2024

PROGRESIÓN SOCIEDAD COMISIONISTA DE BOLSA S.A

Tabla de contenido

ESTAMENTOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN 3
Definición de seguridad de la información 3
Objetivos generales del documento 3
Justificación 3
Alcance del documento 3
Organización general del documento 4
Responsable 4
Contacto 4
Procedimiento para solicitar excepciones 5
Declaración directiva 5
Declaración de aprobación 6
Definiciones 6
Referencias y otros documentos 8
POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 8
Declaración de la política general de seguridad de la información 8
Objetivo de la política de seguridad de la información 8
Alcance de la política de seguridad de la información 8
Roles y responsabilidades 9
POLÍTICAS DE LA ORGANIZACIÓN PARA PRESERVAR LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 10
A6. Política de organización de la seguridad de la información y ciberseguridad 10
A7. Política de seguridad de los recursos humanos 11
A8. Política de gestión de activos 12
A9. Política de control de acceso 13
A10. Política de política de criptografía. 14
A11. Política de seguridad física y del entorno 15
A12. Política de gestión de comunicaciones y operaciones 16

A14. Política de adquisición, desarrollo y mantenimiento de sistemas de información 17
A16. Política de gestión de incidentes de seguridad..... 18
A17. Política de continuidad del negocio..... 19
Esquema de severidad y sanciones..... 20

ESTAMENTOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN

Definición de seguridad de la información

La seguridad de la información consiste en preservar la confidencialidad, la integridad y la disponibilidad de la información que se maneja a través y dentro de Progresión Sociedad Comisionista de Bolsa S.A (en adelante Progresión SCB); de la misma manera busca preservar el buen uso de los activos de información a través de la autenticidad, trazabilidad, aceptación y fiabilidad de su uso.

Objetivos generales del documento

Preservar la vigencia, aplicabilidad, pertinencia y difusión de las políticas de seguridad de la información y ciberseguridad al interior de la compañía.

Justificación

1. Siguiendo las directrices entregadas por la Norma Internacional ISO 27001:2022 se establecen lineamientos que guíen a Progresión SCB a una adecuada protección de los activos de información.
2. Bajo la premisa de la documentación de las actividades dentro de la organización para preservar su existencia, se diseña un documento que contenga las políticas de seguridad y ciberseguridad, el cual será objeto de revisiones y actualizaciones.
3. Buscando la difusión de las políticas de seguridad dentro del personal de la organización se utiliza una herramienta que garantice su consistencia, aplicabilidad y difusión.

Alcance del documento

Este documento comprende todas las políticas de seguridad de la información aplicables y vigentes para Progresión SCB y un esquema de severidad y sanciones que ayuda a asegurar el correcto cumplimiento de éstas.

Organización general del documento

Este documento está compuesto por cuatro (4) secciones principales que el lector deberá tener en cuenta para hacer una correcta interpretación de este:

Sección	Contenido
ESTAMENTOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN	En esta sección se encuentran contenidos, estamentos generales que permiten al lector entender el significado y la dirección de Progresión SCB en cuanto a la seguridad de la información. Dentro de este se encuentra el marco conceptual necesario para interpretar correctamente las políticas de la seguridad de la información y ciberseguridad.
POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	En esta sección se describe la política principal o general de seguridad de la información y ciberseguridad, de la cual se desprenden o generan el resto de las políticas, controles, estándares y procedimientos orientados a la protección de los activos de información. Esta política de obligatorio cumplimiento refleja la dirección que Progresión SCB busca con el fin de proteger la información suya y la de sus clientes, y generar valor a partir del uso adecuado de ella.
POLÍTICAS DE LA ORGANIZACIÓN PARA PRESERVAR LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	En esta sección se encuentra una serie de políticas que se desprenden de la política general de la seguridad de la información y ciberseguridad y las cuales buscan reflejar la dirección de Progresión SCB en diferentes áreas de información de la organización. Estas políticas, al igual que la política general, son de obligatorio cumplimiento, y la falta a una de ellas, tiene sanciones asociadas. La sanción aplicada como resultado de una falta a la política se describe en cada una de estas. El detalle de cada sanción se encuentra en la sección D. SEVERIDAD Y SANCIONES.
SEVERIDAD Y SANCIONES	En esta sección se encuentran relacionadas para cada uno de los niveles de severidad definidos una sanción asociada a ellos.

Responsable

El Oficial de ciberseguridad y seguridad de la información y la alta dirección de Progresión SCB, velara por el cumplimiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad; y sus políticas de seguridad de la información, así como de su vigencia, pertinencia, mantenimiento y divulgación dentro de la organización.

Contacto

En caso de tener alguna duda u observación con respecto al presente documento debe comunicarse con el responsable del Sistema de Gestión de Seguridad de la Información y Ciberseguridad al:

Teléfono: 3905591 Ext. 488
E-mail: ciberseguridad@progresion.com.co
Dependencia: Ciberseguridad y Seguridad de la información

Procedimiento para solicitar excepciones

Si usted es un funcionario de Progresión SCB o tiene alguna relación con la organización y encuentra alguna excepción o situación particular en la cual se dificulte o se imposibilite el cumplimiento de alguna política de seguridad de la información o ciberseguridad de manera temporal o definitiva por causas naturales, humanas o económicas, puede solicitar una excepción temporal o definitiva para el cumplimiento de dicha política según el siguiente Instructivo:

Deberá enviar un correo electrónico documentando el caso completo y el porqué de la excepción al Oficial de ciberseguridad y seguridad de la información el cual realizará el debido trámite con el área de Control Interno. Esta solicitud debe incluir:

- Su nombre y apellido
- Número de cédula
- Empresa donde labora
- Relación con Progresión SCB
- Cargo o labor que desempeña
- Dependencia a la cual pertenece
- Lugar en donde lleva a cabo su labor
- Política en la cual ocurre la excepción
- Motivo de la excepción
- Fecha de solicitud de la excepción

Se le dará repuesta a su solicitud en un plazo no mayor a 30 días hábiles. En caso de que esto no ocurra, puede realizar el mismo procedimiento para comunicarse con el Líderes de procesos organizacionales de Auditoría en las oficinas de Progresión SCB, la cual tendrá un plazo no mayor a 30 días hábiles para responderle y su estado puede ser consultado en que se encuentre dicha solicitud en cualquier momento.

En el evento en que se deba aplicar la excepción antes de que se cumpla el tiempo estimado de aprobación por parte del Líderes de procesos organizacionales de Auditoría, se debe solicitar permiso para incurrir en el incumplimiento de la política al jefe inmediato.

Declaración directiva

Progresión SCB es una compañía del sector financiero que busca ofrecer productos y servicios que garanticen satisfacer las expectativas de los clientes, la preservación de la integridad, disponibilidad y confidencialidad de la información de estos, así como la continuidad del negocio que soporta los servicios ofrecidos a los mismos, buscando que dicho servicio sea oportuno y personalizado, apoyado en herramientas de alta tecnología y en la gestión proactiva de los riesgos, generando así confianza en la gestión que se tiene sobre la operación de la organización y la seguridad de la información y ciberseguridad que ella requiere.

En la compañía Progresión SCB se cuenta con un equipo de profesionales capacitado, comprometido y apoyado en el aseguramiento de los activos de información, a través de la constante formación y sensibilización del personal, así como la divulgación y retroalimentación de los riesgos e impactos identificados dentro de la organización.

La dirección de Progresión SCB se encuentra alineada con esta política integrada y se responsabilizará de su correcta difusión e implementación al interior de la organización.

Declaración de aprobación

De maneara unánime los señores directores (100% del cuórum presente), declara que las políticas de seguridad de la información y ciberseguridad buscan la disminución, a un nivel aceptable de los riesgos a los que está expuesta la información de la organización y que están alineadas con la misión y visión que tiene Progresión SCB para con sus clientes.

Declara, que el documento de políticas de seguridad de la información y ciberseguridad entra en vigor a partir del 2 de septiembre del 2024 y que es de obligatorio cumplimiento para todos los funcionarios de Progresión SCB, contratistas, proveedores, consultores y cualquier otro tipo de terceros que desempeñen funciones en las oficinas de la compañía y/o que el desempeño de sus labores esté relacionado con activos de información de Progresión SCB.

Esta política se divulgará y/o dará a conocer a empleados, contratistas, proveedores y consultores y se contraerán acuerdos que obliguen al cumplimiento de ésta.

Junta Directiva
Acta N° 456 - 26/08/2024

Definiciones

#	Término	Definición
1	Información	Son datos que poseen significado (ISO 9000 numeral 3.7.1)
2	Activos de información	Se refiere a información o activos que procesan datos como por ejemplo: las personas, los sistemas, los servicios, la imagen corporativa y las aplicaciones.
3	Política de SI	Son documentos de alto nivel que representan la filosofía corporativa y el pensamiento estratégico de los directivos en cuanto a la seguridad de la información, con el fin de desarrollar controles en un área definida sobre los sistemas de información y los recursos relacionados. Su violación o incumplimiento lleva a la aplicación de sanciones.
4	Estándar de SI	Son especificaciones de SI sobre sistemas o procedimientos específicos que tienen que ser cumplidos por todos dentro de la organización. Son orientaciones obligatorias que buscan hacer cumplir las políticas.
5	Procedimiento de SI	Son documentos secuenciales detallados, derivados de las políticas de SI que implementan el espíritu de estas, de modo que sean fácilmente comprendidos por todos los que se deben regir por ellos. Los procedimientos definen específicamente cómo las políticas, estándares, mejores prácticas y lineamientos serán implementados en una situación dada.
6	Lineamiento o guía de SI	Es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas de SI.
7	Mejor Práctica de SI	Es una regla de seguridad específica a una plataforma o problema en particular, que es aceptada a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta.
8	Norma	Son especificaciones técnicas de aplicación voluntaria, elaboradas por consenso de los interesados, y que son aprobadas por un organismo nacional, regional o internacional de normalización reconocido
9	Ley	Es un estamento mandatorio que dicta el gobierno de un país y que debe ser cumplido por las organizaciones que sean cobijadas por ella.
10	SGSI	Sistema de gestión de la seguridad de la información
11	Disponibilidad	Es un atributo de la seguridad de la información que indica que ésta siempre debe

		estar accesible sólo para las personas autorizadas.
12	Confidencialidad	Es un atributo de la seguridad de la información que indica que la información solo debe poder ser accedida por las personas autorizadas.
13	Integridad	Es un atributo de la seguridad de la información que indica que la información solo puede ser modificada por las personas autorizadas.
14	Autenticación	Es un mecanismo necesario para garantizar que se conserven los atributos de la seguridad de la información que implica que se reconozca la identidad de un usuario que desea acceder a un servicio o información.
15	Autorización	Es un mecanismo necesario para garantizar los atributos de la seguridad de la información que indica qué usuarios identificados tienen permiso para acceder a un recurso o información.
16	Severidad	Hace referencia a una escala que mide qué tan grave es la falta o violación a una política de la organización.
17	Sanción	Es una pena o castigo que se impone por la falta o violación a una política de la organización.
18	Propósitos legítimos	Se entiende por propósitos legítimos toda actividad que esté relacionada con cumplir los objetivos de negocio y que se encuentra dentro de la ley.
19	Incidente de seguridad de la información	Está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de poner en peligro las operaciones del negocio y amenazar la seguridad de la información.
20	Evento de seguridad de la información	Es la presencia identificada de un estado del sistema, del servicio o de la red que indica un incumplimiento posible de la política de seguridad de la información, una falla de las salvaguardas, o una situación previamente desconocida que puede ser pertinente para la seguridad.
21	Documentos organizacionales	Información (datos que poseen significado) y su medio de soporte. Ejemplo: Registro, especificación, procedimiento documentado, plano, informe, norma. Nota 1: El medio de soporte puede ser papel, disco magnético, óptico o electrónico, fotografía o muestra patrón o una combinación de éstos. Nota 2: Con frecuencia, un conjunto de documentos, por ejemplo, especificaciones y registros, se denominan "documentación".
22	Código móvil	El código móvil es un código de software que transfiere de una computadora a otra computadora y luego ejecuta automáticamente y realiza una función específica con muy poca o ninguna interacción.
23	Código malicioso	Cualquier conjunto de códigos, especialmente sentencias de programación, que tiene un fin malicioso. Esta definición incluye tanto programas malignos compilados, como macros y códigos que se ejecutan directamente, como los que suelen emplearse en las páginas web (scripts).
24	Progresión SCB	Progresión Sociedad Comisionista de Bolsa S.A.

Referencias y otros documentos

- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information technology – Security techniques – Code of practice for information security management. Geneva: ISO 27001:2022 – ISO 27002.
- BRITISH STANDARDS INSTITUTION. Business Continuity Management. London, BSI. (BS 25999-2:2008).

POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Declaración de la política general de seguridad de la información

La organización es una compañía del sector Financiero, Comisionista de Bolsa que busca el cumplimiento de los requisitos relacionados con la seguridad de la información y la ciberseguridad, buscando que productos y servicios se apoyen en una gestión proactiva de los riesgos.

La organización ofrece su servicio de Comisionista de Bolsa apoyada en un equipo de profesionales preparado para procurar el aseguramiento de los activos de información, a través de la constante formación y sensibilización del personal, así como la divulgación y retroalimentación de los riesgos e impactos identificados dentro de la organización.

La alta dirección de Progresión SCB se encuentra alineada con esta política integrada y se responsabilizará de su correcta difusión e implementación al interior de la organización.

Objetivo de la política de seguridad de la información

Asegurar que la información de Progresión SCB y la depositada en ella por sus clientes, proveedores, contratistas, empleados y consultores sea usada de la manera en que fue pensada para el beneficio de sus clientes, empleados y demás interesados.

Alcance de la política de seguridad de la información

La política general de seguridad de la información debe ser cumplida por todos los empleados y directivos de Progresión SCB, proveedores, consultores y cualquier otro tipo de terceros que desempeñen funciones en las instalaciones de Progresión SCB y/o que el desempeño de sus labores esté relacionado con activos de información de la comisionista.

Roles y responsabilidades

#	Rol	Responsabilidades
1	Empleados	Cumplir con la política general de seguridad de la información y seguir los estándares, procedimientos, lineamientos y buenas prácticas que permitan asegurar la información de Progresión SCB y/o reducir el riesgo de pérdida de su seguridad a un nivel aceptable para la organización. Los empleados también son responsables de denunciar cualquier mal uso, desviación o falta a la política y/o que comprometa la seguridad de la información de Progresión SCB.
2	Directores	Asegurar que los miembros de su equipo de trabajo cumplan con la política general de seguridad de la información. Motivar la difusión y el conocimiento de la política general de seguridad de la información al interior de su área y realizar una evaluación constante de ello.
3	Responsables de proceso	Implementar controles, estándares y procedimientos derivados de la política general de seguridad de la información que aseguren su cumplimiento dentro de su proceso.
4	Responsable de proceso de Gestión de Seguridad de la Información	El Proceso de Gestión de Seguridad de la Información tiene la responsabilidad de implementar la política al interior de Progresión SCB.
5	Responsable de proceso de Administración de la infraestructura	Gestionar incidentes relacionados con la violación a la política general de seguridad de la información.
6	Líderes de procesos organizacionales de Auditoría	Verificar el correcto cumplimiento de la política general de seguridad de la información de Progresión SCB.
7	Terceros y otras personas relacionadas con la organización	Cumplir con la política de seguridad que aplican a la relación que tengan estos con Progresión SCB para conservar la seguridad de la información a la cual tienen acceso ambas partes.

POLÍTICAS DE LA ORGANIZACIÓN PARA PRESERVAR LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

A6. Política de organización de la seguridad de la información y ciberseguridad

1. Nombre de la política: Política de organización de la seguridad de la información y ciberseguridad.
2. Definición completa: La alta dirección de Progresión SCB evidencia su compromiso con relación a la seguridad de la información, a través de la asignación de responsabilidades a los empleados, contratistas, proveedores y partes interesadas, adicionalmente velara por que se entreguen permisos para acceder a los servicios de procesamiento de información.
   Los empleados, contratistas, proveedores y partes interesadas que tengan acceso a los activos de información de Progresión SCB deberán firmar acuerdos de confidencialidad, de esta misma manera los riesgos asociados a cada uno de ellos serán identificados y se implementaran controles para evitar la materialización de estos.
   Los empleados, contratistas, proveedores y partes interesadas que tengan acceso a los activos de información de Progresión SCB no deben suministrar información alguna de la entidad, de los clientes, empleados o terceros a ningún ente externo sin las autorizaciones respectivas.
3. Público objetivo al que va dirigido(a): Empleados, proveedores, contratistas, consultores y externos.
4. Regulación: ISO 27001:2022 – ISO 27002 Capítulo A6
5. Implicaciones:
   - La dirección apoyará activamente la seguridad de la información dentro de la organización.
   - Las actividades relacionadas con seguridad de la información deben incluir personal de toda la organización.
   - Se definirán las responsabilidades con relación a la seguridad de la información para los empleados, contratistas, proveedores y partes interesadas asociados a la organización.
   - La autorización para nuevos servicios de procesamiento de información debe ser entregada directamente por la alta dirección.
   - Se contará con acuerdos de confidencialidad orientados a la no divulgación de la información que se maneja al interior de la organización.
   - Se mantendrá contacto con grupos de interés que ayuden a la organización a estar actualizada con relación a la seguridad de la información.
   - Dentro del proceso de gestión de riesgos se tendrán en cuenta los riesgos asociados a empleados, contratistas, proveedores y partes interesadas.
   - Se realizarán revisiones al proceso de Gestión de Seguridad de la información y ciberseguridad de manera periódica por parte de un tercero independiente.
6. Roles y responsabilidades:
   - Usuarios:
     - Cumplir con esta política y con los estándares, procedimientos y buenas prácticas que tenga la organización para el buen uso de los recursos tecnológicos.
   - Líderes de procesos organizacionales:
     - Proveer los recursos necesarios para que esta política sea cumplida.
     - Auditar sobre el cumplimiento de esta política.
     - Conservar la vigencia de los estándares y procedimientos que apoyen el cumplimiento de esta política.
     - Definir cuáles son las características de buen uso de los recursos tecnológicos y los sitios desde los cuales es seguro usarlos
     - Hacer revisiones periódicas sobre los sistemas para asegurar el buen cumplimiento

de esta política.

7. Severidad: Grave

A7. Política de seguridad de los recursos humanos

1. Nombre de la política: Política de seguridad de los recursos humanos.
2. Definición completa: Los roles y responsabilidades con relación a la seguridad de la información deben ser identificados con base en los activos de información que serán utilizados, y serán divulgados a través de los contratos de los empleados, proveedores contratistas, y consultores que tengan acceso a los activos de información de Progresión SCB, su cumplimiento será vigilado por la alta dirección, quien mostrará su compromiso con la seguridad de la información a través de la verificación de la identificación, divulgación y aceptación de dichos roles y responsabilidades.

   El incumplimiento de las políticas de seguridad de la información diseñadas por Progresión SCB iniciara la aplicación de un proceso disciplinario sobre el empleado, contratista o usuario de tercera parte que incurra en la falta de la política.
3. Público objetivo al que va dirigido(a): Empleados, proveedores, contratistas, consultores y externos.
4. Regulación: ISO 27001:2022 – ISO 27002 Capítulo A7
5. Implicaciones:
   - Deben estar documentados los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes con relación a la seguridad de la información.
   - Todo empleado, contratista y usuario de tercera parte debe conocer sus roles y responsabilidades con relación a la seguridad de la información.
   - Deben existir reglamentos claros y estamentos organizacionales asociados a la contratación del personal con base en la criticidad del cargo y su contacto con la información confidencial.
   - Definición de términos y condiciones laborales que establezca la responsabilidad del cargo y de la organización con relación a la seguridad de la información.
   - Se brindará a los empleados de la organización y cuando sea pertinente, los contratistas y usuarios de terceras partes educación, formación y concientización sobre la seguridad de la información.
   - Se solicitará sean firmados acuerdos de confidencialidad por parte de los empleados y dicho acuerdo de confidencialidad se encontrará asociado a una penalidad específica.
   - Cuando aplique el cambio o terminación de la contratación laboral debe estar debidamente documentado y se deben asignar las responsabilidades para llevarlos a cabo.
   - Los activos pertenecientes a la organización deben ser regresados a esta una vez se haya terminado el contrato laboral, contrato o acuerdo para el cual estaban siendo utilizados.
   - Los derechos de acceso de los empleados, contratistas y usuarios de terceras partes a los activos de información deben ser suspendidos al momento en que se lleve a cabo un cambio o terminación del contrato laboral, contrato o acuerdo.
   - Durante el proceso de selección del personal, contratistas y proveedores se realizará la verificación de los antecedentes de los candidatos, los cuales deben conocer y aceptar sus responsabilidades con relación a la seguridad de la información manejada a través y por Progresión SCB.
   - Cuando se termine el contrato ya sea laboral o contractual deben ser retirados todos los privilegios asignados, se deben entregar los activos de información suministrados y retirar los derechos de acceso a los activos de información de Progresión SCB.
6. Roles y responsabilidades:
   Usuarios:
   - Cumplir con esta política y con los estándares, procedimientos y buenas prácticas que tenga la organización para el buen uso de los recursos tecnológicos.

Responsables del proceso de Gestión Administrativa:

- Incluir dentro del proceso de inducción la asignación de las responsabilidades asociadas a seguridad de la información.
- Diseñar reglamentos para la contratación del personal con base en su impacto sobre la seguridad de la información.
- Exigir la firma de los acuerdos de confidencialidad al momento de una contratación.
- Documentar las actividades a seguir cuando se lleve a cabo un cambio o terminación de contrato laboral, contrato o acuerdo.

Líderes de procesos organizacionales de Gestión de Seguridad de la Información:

- Proveer los recursos necesarios para que esta política sea cumplida.
- Auditar sobre el cumplimiento de esta política.
- Conservar la vigencia de los estándares y procedimientos que apoyen el cumplimiento de esta política.
- Hacer revisiones periódicas sobre los sistemas para asegurar el buen cumplimiento de esta política.

7. Severidad: Grave.

A8. Política de gestión de activos

1. Nombre de la política: Política de gestión de activos.
2. Definición completa: Es deber de los empleados, contratistas, clientes, proveedores y consultores que tengan contacto con activos de información de Progresión SCB protegerlos, así como utilizarlos para el desempeño de sus funciones únicamente. El buen uso de dichos activos de información debe estar asociado a una proactiva gestión en la identificación de las amenazas y vulnerabilidades a las cuales se encuentran expuestas dichos activos de información, así como la implementación de controles que los protejan, buscando el uso adecuado de los mismos.
   Adicionalmente se preservará la protección, clasificación, etiquetado y adecuado manejo de la información confidencial con la cual se tenga contacto durante el uso de los activos de información.
3. Público objetivo al que va dirigido(a): Empleados, proveedores, contratistas, consultores y externos.
4. Regulación: NTC ISO 27001:2022 – ISO 27002 Capítulo A8.
5. Implicaciones:
   - El uso adecuado de los activos de información de la organización está limitado a los objetivos para los cuales la organización los tiene destinados, no para usos personales.
   - Es responsabilidad de los usuarios proteger las características de seguridad de la información de los activos de información que estén relacionados con el desempeño de sus labores.
   - Los procesos de la organización serán responsables de definir los lineamientos del buen uso de la información generada o procesada a través de estos.
   - Se deben comunicar las amenazas y vulnerabilidades identificadas por los empleados, contratistas, clientes, proveedores y consultores que tengan contacto directo con los activos de información de Progresión SCB.
   - Seleccionar e implantar controles para mitigar o eliminar las vulnerabilidades identificadas por los empleados, contratistas, clientes, proveedores y consultores que de Progresión SCB.
   - Existencia de políticas enfocadas al buen uso de los activos de información propiedad y responsabilidad de Progresión SCB.
   - Realización de procedimientos que garanticen el bueno uso de los activos de información propiedad y responsabilidad de Progresión SCB.
   - Estudio y selección de estándares y buenas prácticas internacionales que busquen preservar las características de la información de los activos de información propiedad y responsabilidad de Progresión SCB.
   - Ningún empleado estará autorizado para involucrarse en alguna actividad fuera de la ley haciendo uso de los recursos tecnológicos de la organización.

- Se clasificará la información y será etiquetada con base en dicha clasificación, con el fin de brindarle un adecuado manejo a esta.
- No se permitirá la instalación de programas con código malicioso en los equipos de la organización.
- No está permitido compartir credenciales de acceso a los recursos tecnológicos de la organización.
- El uso de la mensajería electrónica debe estar sujeto a los propósitos de la organización y cualquier desviación sobre éste que comprometa la seguridad de la información de la organización está completamente prohibido.
- Se debe evitar siempre hacer uso de los recursos tecnológicos de la organización para convertirse en generador de amenazas para terceros por dentro y fuera de la organización.
- Todos los usuarios deberán usar las herramientas tecnológicas únicamente desde los sitios que la organización ha declarado seguros y ha aprobado el uso de estos.
- Monitorear el tráfico de red de los usuarios que acceden desde la casa por medio de VPN.

6. Roles y responsabilidades:
   Usuarios:
   - Cumplir con esta política y con los estándares, procedimientos y buenas prácticas que tenga la organización para el buen uso de los recursos tecnológicos.

   Líderes de procesos organizacionales:
   - Proveer los recursos necesarios para que esta política sea cumplida.
   - Auditar sobre el cumplimiento de esta política.
   - Conservar la vigencia de los estándares y procedimientos que apoyen el cumplimiento de esta política.
   - Definir cuáles son las características de buen uso de los recursos tecnológicos y los sitios desde los cuales es seguro usarlos.
   - Hacer revisiones periódicas sobre los sistemas para asegurar el buen cumplimiento de esta política.
7. Severidad: Grave.

A9. Política de control de acceso

1. Nombre de la política: Política de control de acceso.
2. Definición completa: Las instalaciones de Progresión SCB serán protegidas con base en la criticidad de los activos de información que se encuentren en estas, se debe gestionar el acceso de los usuarios a la información a través de los activos de información, asignando la responsabilidad que cada usuario tiene frente a dichos permisos con relación a las redes, los sistemas operativos, y las aplicaciones e información contenida en estos. Cuando un empleado, contratista, proveedor o tercera parte que necesite realizar trabajos remotos se aplicarán controles orientados a la preservación de las características de la seguridad de la información, de igual forma se controlarán los dispositivos de computación y comunicaciones móviles.
3. Público objetivo al que va dirigido(a): Empleados, proveedores, contratistas, consultores y externos.
4. Regulación: NTC ISO 27001:2022 – ISO 27002 Capítulo A9.
5. Implicaciones:
   - Se tendrá un estricto control de acceso a las instalaciones y a los activos de información de Progresión SCB.
   - Los usuarios deben contar con permisos y contraseñas asignadas por el proceso de Gestión de Acceso, para los cuales deben haber contado con la autorización expresa de su jefe inmediato.
   - Las contraseñas son individuales y no deben imprimirse, almacenarse en línea o compartirse con otras personas.
   - Los usuarios son responsables de todas las transacciones y movimientos que se realicen con

sus contraseñas.
- Los usuarios deberán proporcionar la seguridad y complejidad adecuada de sus contraseñas.
- Cuando se asignen privilegios a los usuarios estos deberán estar avalados por su jefe inmediato.
- Los derechos de acceso serán revisados periódicamente por el proceso de Gestión de Acceso.
- Las contraseñas deben ser cambiadas por parte de los usuarios cada tiempo y su complejidad deberá ser con base en las directrices de Progresión SCB.
- Los usuarios serán responsables de sus equipos y buscarán protección para los equipos de usuario desatendidos.
- Los usuarios serán responsables de mantener el escritorio y la pantalla despejada para los activos de información a través de los cuales se realiza procesamiento de información.
- Los usuarios tendrán acceso solo a los servicios para cuyo uso están autorizado, y se controlara el acceso de usuarios remotos a dichos servicios.
- Se controlará el acceso tanto lógico como físico a los puertos de configuración y de diagnóstico.
- Se suspenderán las sesiones inactivas después de 5 minutos con el fin de proteger las características de la información.
- Se prohíbe el acceso de los usuarios que utilizan el servicio de internet de la compañía, a las siguientes páginas web:
    - Que permitan el intercambio de información.
    - Redes sociales (que no estén previamente autorizadas)
    - Contenido para adulto.
    - Potencialmente responsable
    - Descarga de software

6. Roles y responsabilidades:
   Usuarios:
   - Cumplir con esta política y con los estándares, procedimientos y buenas prácticas que tenga la organización para el buen uso de los recursos tecnológicos.

   Líderes de procesos organizacionales de Gestión de Seguridad de la Información:
   - Proveer los recursos necesarios para que esta política sea cumplida.
   - Auditar sobre el cumplimiento de esta política.
   - Conservar la vigencia de los estándares y procedimientos que apoyen el cumplimiento de esta política.
   - Auditar el control de acceso a los sistemas operativos, aplicaciones y la información.
   - Hacer revisiones periódicas sobre los sistemas para asegurar el buen cumplimiento de esta.
   - Definir con ayuda de las áreas cuales son los procedimientos operacionales y las responsabilidades frente a estos por parte de los empleados directamente relacionados con estos.
   - Hacer revisiones de los controles aplicados a las terceras partes con relación al servicio que prestan a la organización.
7. Severidad: Grave.

A10. Política de política de criptografía.

1. Nombre de la política: Política de criptografía.
2. Definición completa: Las medidas de control para el uso eficaz de la criptografía para proteger la confidencialidad e integridad de la información según las directrices de ISO 27001
3. Público objetivo al que va dirigido(a): Empleados, proveedores, contratistas, consultores y externos.
4. Regulación: NTC ISO 27001:2022 – ISO 27002 Capítulo A10.
5. Implicaciones:

- Los controles criptográficos deben estar enfocados a la protección de la información en el caso de que un intruso pueda tener acceso físico a la información sensible.
- Se debe establecer un sistema de cifrado de la misma para dificultar la violación de su confidencialidad o su integridad.
- Se debe establecer que información y en qué circunstancias será necesario aplicar claves criptográficas.
- Se debe determinar las fechas de activación y desactivación de claves.
- Se debe tener complejidad en las claves usadas por los Empleados, proveedores, contratistas, consultores y externos.

6. Roles y responsabilidades:
   Usuarios:
   - Cumplir con esta política y con los estándares, procedimientos y buenas prácticas que tenga la organización para el buen uso de los recursos tecnológicos.

   Líderes de procesos organizacionales de Gestión de Seguridad de la Información:
   - Proveer los recursos necesarios para que esta política sea cumplida.
   - Auditar sobre el cumplimiento de esta política.
   - Conservar la vigencia de los estándares y procedimientos que apoyen el cumplimiento de esta política.
   - Auditar el control de acceso a los sistemas operativos, aplicaciones y la información.
   - Hacer revisiones periódicas sobre los sistemas para asegurar el buen cumplimiento de esta.
   - Definir con ayuda de las áreas cuales son los procedimientos operacionales y las responsabilidades frente a estos por parte de los empleados directamente relacionados con estos.
   - Hacer revisiones de los controles aplicados a las terceras partes con relación al servicio que prestan a la organización.
7. Severidad: Grave.

A11. Política de seguridad física y del entorno

1. Nombre de la política: Política de seguridad física y del entorno.
2. Definición completa: A través de la implantación de controles de acceso físicos Progresión SCB velara por un perímetro de seguridad física seguro, estos controles estarán orientados a salvaguardar la seguridad y la continuidad de las operaciones de las oficinas, recintos e instalaciones en donde se encuentran los activos de información propiedad y administrados por la organización.
3. Público objetivo al que va dirigido(a): Empleados, proveedores, contratistas, consultores y externos.
4. Regulación: NTC ISO 27001:2022 – ISO 27002 Capítulo A11.
5. Implicaciones:
   - Se tendrán documentados los procedimientos para el control de acceso a las instalaciones de la organización.
   - Todo empleado, contratista y usuario de tercera parte debe atender esta política.
   - Dentro del reglamento de los empleados debe estar explicito que el retiro de los activos de información es responsabilidad directa de ellos y que se requiere permiso del jefe inmediato para retirarlo de las instalaciones de Progresión SCB.
   - Definición de términos y condiciones laborales que establezca la responsabilidad del cargo y de la organización con relación a los activos de información.
   - Se contará con controles de acceso físicos estrictos por parte del personal de seguridad que permite el acceso a las instalaciones a personal externo a la organización.
6. Roles y responsabilidades:

Usuarios:

- Cumplir con esta política y con los estándares, procedimientos y buenas prácticas que tenga la organización para el buen uso de los recursos tecnológicos.

Responsables del proceso:

- Verificar que se cumplan los lineamientos de seguridad física entregados por la alta dirección para el ingreso y salida de activos de información y usuarios, de las instalaciones de la organización.
- Velar por que se reporten los incidentes de seguridad asociados a seguridad física.
- Garantizar que se cuenta con los recursos suficientes para aplicar esta política.

7. Severidad: Grave.

A12. Política de gestión de comunicaciones y operaciones

1. Nombre de la política: Política de gestión de comunicaciones y operaciones.
2. Definición completa: Los empleados, proveedores, contratistas y consultores son responsables de velar por el correcto desarrollo de las comunicaciones y operaciones dentro de la organización a través de la realización y el mantenimiento de documentos de operación, el reporte de los cambios realizados sobre los activos de información utilizado para el desempeño de sus funciones, las cuales deben ser plenamente identificas y comunicadas. Los ambientes de producción, prueba y desarrollo serán utilizados teniendo en cuenta los roles y responsabilidades que se tienen sobre los mismos y se velará por la protección de los activos de información de códigos maliciosos y móviles que puedan ser implantados de manera intencional o accidental, así como la realización del respaldo de la información necesaria para la prestación de los servicios y la correcta ejecución de los procesos.
3. Público objetivo al que va dirigido(a): Empleados, proveedores, contratistas, consultores y externos.
4. Regulación: NTC ISO 27001:2022 – ISO 27002 Capítulo A12.
5. Implicaciones:
    - Se asegurará la operación correcta y segura de los servicios de procesamiento de información.
    - Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.
    - Se controlarán los cambios en los servicios y los sistemas de procesamiento de información.
    - El proceso de gestión de talento humano deberá entregar a los empleados, contratistas, proveedores y terceras partes las funciones y responsabilidades con relación a la seguridad de la información y ciberseguridad.
    - Las pruebas, el desarrollo y la operación de los servicios se deben llevar a cabo en ambientes separados para evitar alteraciones en las características de la información.
    - Se acordarán niveles de servicio con proveedores, contratistas y terceras partes, y estos deben de ser medidos, así como verificados los controles de seguridad, los servicios, los cambios realizados sobre estos que son prestados por dichos proveedores, contratistas y terceras partes.
    - Se implementarán controles para la detección de códigos móviles y maliciosos y se brindará capacitación al personal para ayudarlos a identificarlos.
    - La realización de copias de respaldo de información y software será obligatoria.
    - Las redes serán mantenidas y controladas, los acuerdos sobre los servicios de la red deben identificar e incluir las características de seguridad.
    - El uso de los medios removibles deberá ser autorizado por el líder del proceso de Gestión de Seguridad de la Información, por medio del procedimiento de excepciones.
    - El intercambio de información deberá ser llevado a cabo a través de los procedimientos y

controles formales identificados para su realización.

- La información intercambiada a través de correos electrónicos deberá ser protegida en su confidencialidad, integridad y disponibilidad.
- Se tendrá registro de los incidentes de seguridad en que se incurran, las actividades realizadas por los usuarios y las excepciones para la realización de auditorías.
- Se tendrán registros de fallas asociados a acciones correctivas con el fin de evitar el incurrir nuevamente en estas.
- El uso de los medios removibles por parte de personal no autorizado debe ser reportado como un incidente de seguridad a través del canal adecuado, de esta misma manera se tendrá control sobre el intercambio de información que se realice a través de los activos de información, verificando que dicho intercambio no genere riesgos.

6. Roles y responsabilidades:
   Usuarios:
   - Cumplir con esta política y con los estándares, procedimientos y buenas prácticas que tenga la organización para el buen uso de los recursos tecnológicos.

   Líderes de procesos organizacionales de Gestión de Seguridad de la Información:
   - Proveer los recursos necesarios para que esta política sea cumplida.
   - Auditar sobre el cumplimiento de esta política.
   - Conservar la vigencia de los estándares y procedimientos que apoyen el cumplimiento de esta política.
   - Definir con ayuda de las áreas cuales son los procedimientos operacionales y las responsabilidades frente a estos por parte de los empleados directamente relacionados con estos.
   - Hacer revisiones de los controles aplicados a las terceras partes con relación al servicio que prestan a la organización.
   - Hacer revisiones periódicas sobre los sistemas para asegurar el buen cumplimiento de esta política.
7. Severidad: Grave.

A14. Política de adquisición, desarrollo y mantenimiento de sistemas de información

1. Nombre de la política: Política de adquisición, desarrollo y mantenimiento de sistemas de información.
2. Definición completa: Los sistemas de información deberán cumplir con los requisitos de seguridad de la información identificados en Progresión SCB, y su adquisición, desarrollo o mantenimiento deberán estar alienados con dichos requisitos, los datos de entrada y de salida de los sistemas de información deben mantener su integridad, confidencialidad y disponibilidad, de tal forma que se identificaran datos de prueba con el fin de no exponer datos reales y el acceso al código fuente de las aplicaciones será restringido, se llevarán a cabo validaciones de la operación de las aplicaciones con el fin de evitar que se presenten interrupciones en el servicio.
3. Público objetivo al que va dirigido(a): Empleados, proveedores, contratistas, consultores y externos.
4. Regulación: NTC ISO 27001:2022 – ISO 27002 Capítulo A14.
5. Implicaciones:
   Se deben analizar los requisitos de seguridad asociados a la realización de nuevos sistemas de información y especificar los controles para proteger las características de seguridad de estos.
   - Se tendrán verificaciones de validación en las aplicaciones tanto para sus datos de entrada

como de salida, como para la autenticación e integridad del mensaje.

- La información debe ser encriptada cuando sea necesario y se debe contar con un sistema de gestión de llaves que soporte la encriptación de la información.
- La instalación de software en los sistemas operativos debe realizarse bajo la autorización del líder del proceso de Gestión de Seguridad de la información, y el acceso al código fuente de los programas será restringido.
- Se contará con datos de prueba para la realización de estas diferentes que no contengan información confidencial de la organización.
- Los cambios realizados a los sistemas operativos y las aplicaciones serán controlados, y dichos cambios serán evaluados a través del proceso de Gestión de Riesgos, evitando realizar cambios en las aplicaciones en caso de no ser estrictamente necesario, con el fin de evitar la fuga de información y la continuidad de la operación, en caso tal de que el software sea desarrollado por un tercero, este debe ser supervisado y monitoreado.
- Cuando se detecte una vulnerabilidad técnica se deben tratar a través del proceso de Gestión de Riesgos, y tomar las acciones pertinentes.
- Se tendrán controles orientados a evitar la fuga de información.
- Se contará con un sistema de gestión de llaves que apoye el uso de los controles criptográficos.
- La información que pase a través de las redes de Progresión SCB será protegida a través de controles criptográficos, dichos controles serán soportados por una efectiva gestión de llaves.
- Los cambios realizados sobre las aplicaciones se realizarán con base en un esquema de control de cambios, después del cual se realizará una revisión del funcionamiento de la aplicación.

6. Roles y responsabilidades:
   Usuarios:
   - Cumplir con esta política y con los estándares, procedimientos y buenas prácticas que tenga la organización para el buen uso de los recursos tecnológicos.

   Líderes de procesos organizacionales de Gestión de Seguridad de la Información:
   - Proveer los recursos necesarios para que esta política sea cumplida.
   - Auditar sobre el cumplimiento de esta política.
   - Conservar la vigencia de los estándares y procedimientos que apoyen el cumplimiento de esta política.
   - Gestionar el funcionamiento de los controles criptográficos
   - Verificar los controles implementados para preservar la seguridad de los archivos del sistema
   - Realizar gestión de las vulnerabilidades técnicas.
7. Severidad: Grave.

A16. Política de gestión de incidentes de seguridad

1. Nombre de la política: Política de gestión de incidentes de seguridad.
2. Definición completa: Los incidentes de seguridad de la información que se presenten deberán ser reportados por los empleados, contratistas, proveedores y terceras partes que tengan contacto con los activos de información de la organización con base en los procedimientos establecidos por Progresión SCB, y a través de los canales identificados para dicho fin.
   Estos incidentes de seguridad de la información serán gestionados, buscando identificar vulnerabilidades asociadas a los activos de información y que puedan poner en riesgo la información propiedad y en tránsito, de la organización y sus clientes.
3. Público objetivo al que va dirigido(a): Empleados, proveedores, contratistas, consultores y externos.

4. Regulación: NTC ISO 27001:2022 – ISO 27002 Capítulo A16.
5. Implicaciones:
    - Se deben reportar todos los incidentes de seguridad de la información, a través de los canales designados por la alta dirección y bajo los procedimientos establecidos a través del proceso de gestión de incidentes.
    - Se reportarán las debilidades detectadas en la seguridad de la información asociadas a los activos de información de la organización.
    - Se brindará una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información reportados por los empleados, contratistas, proveedores y terceras partes.
    - Se cuantificarán y monitorearán todos los incidentes de seguridad de la información con el fin de entregarle a la organización información confiable para realizar la selección de controles necesarios para garantizar las características de la seguridad de la información.
    - Se aplicará el esquema de severidad y sanciones en caso tal de que el incidente de seguridad así lo amerite.
6. Roles y responsabilidades:
   Usuarios:
    - Cumplir con esta política y con los estándares, procedimientos y buenas prácticas que tenga la organización para el buen uso de los recursos tecnológicos.

   Líderes de procesos organizacionales de Gestión de Seguridad de la Información:
    - Proveer los recursos necesarios para que esta política sea cumplida.
    - Auditar sobre el cumplimiento de esta política.
    - Conservar la vigencia de los estándares y procedimientos que apoyen el cumplimiento de esta política.

   Líderes de procesos organizacionales de Gestión de incidentes:
    - Comunicar la política a los responsables de gestionar los incidentes de seguridad de la información.
    - Realizar seguimiento a la gestión prestada sobre los incidentes de seguridad de la información.
7. Severidad: Grave.

A17. Política de continuidad del negocio

1. Nombre de la política: Política de continuidad del negocio.
2. Definición completa: La gestión de la continuidad del negocio será parte integral de la cultura organizacional cumpliendo con los requisitos reglamentarios y garantizando la operación de Progresión SCB, protegiendo y preservando la información de los clientes, a través de la generación de Backups, identificación e implantación de estrategias de continuidad del Negocio, implementación de planes de continuidad del negocio y la realización de pruebas periódicas de dichos planes con el fin de verificar su correcto funcionamiento.
3. Público objetivo al que va dirigido(a): Empleados, proveedores, contratistas, consultores y externos.
4. Regulación: NTC ISO 27001:2022 – ISO 27002 Capítulo A17.
5. Implicaciones:
    - Se contará con un proceso de Gestión para la Continuidad del Negocio.
    - Identificación de amenazas y vulnerabilidad de la organización que se traduzcan en interrupciones a la operación de los servicios.
    - Se asegurará la disponibilidad de la información en el grado y la escala de tiempo requerida por la organización y sus usuarios.
    - Se contará con planes de continuidad del negocio en un mismo formato que sean de fácil

actualización, utilización y ubicación.

- Se realizarán Backups de la información que sea pertinente para mantener la operación del negocio y la prestación del servicio.
- Se llevará a cabo la simulación de escenarios de ciberseguridad funcionales en ambientes controlados con base en su criticidad para la organización y el servicio prestado a los clientes al menos dos veces al año. Estas pruebas deben simular incidentes cibernéticos relevantes y realistas que puedan afectar la operación de los servicios de la organización.
- Los resultados de las pruebas de contingencia se utilizarán para evaluar y actualizar los planes de identificación, contención y respuesta ante incidentes cibernéticos. Se revisarán y ajustarán los procedimientos y estrategias de acuerdo con los hallazgos y lecciones aprendidas durante las simulaciones.
- Los resultados de las pruebas de contingencia deberán ser presentados a la Junta Directiva dentro de los informes semestrales de gestión.

6. Roles y responsabilidades:
   Usuarios:
   - Cumplir con esta política y con los estándares, procedimientos y buenas prácticas que tenga la organización para el buen uso de los recursos tecnológicos.

   Líderes de procesos organizacionales de Gestión de Continuidad del Negocio:
   - Proveer los recursos necesarios para que esta política sea cumplida.
   - Auditar sobre el cumplimiento de esta política.
   - Conservar la vigencia de los estándares y procedimientos que apoyen el cumplimiento de esta política.
   - Verificar la realización de los planes de continuidad, la ejecución de pruebas sobre los mismos y la actualización de estos.
   - Supervisar la realización de los Backups.
   - Programar el mantenimiento de los planes de continuidad del negocio.
7. Severidad: Graves.

Esquema de severidad y sanciones

#	Severidad	Descripción	Sanción
1	Leves	Son faltas leves el incumplimiento de alguna de las políticas establecidas por la Junta Directiva, la administración o el reglamento interno de trabajo, y siempre y cuando no afecte económicamente el patrimonio de la sociedad comisionista ni el de los clientes.	Memorando Interno: comunicado de alerta, sugerencia u oportunidad de mejora, no tiene marca en la hoja de vida, pero se convierte en un soporte de seguimiento ante potenciales acciones que constituyan faltas laborales
2	Graves	Son faltas graves aquellas que, sin que necesariamente sean intencionales, causen algún daño moral o material a la sociedad, socios, empleados o clientes. También es considerada falta grave la reiteración de una falta leve por segunda vez	Llamado de atención por escrito con copia a la hoja de vida.