POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

TABLA DE CONTENIDO

1 OBJETIVO/ PRINCIPIOS ORIENTADORES

El objetivo de la Política de Seguridad de la Información y Ciberseguridad de Seguros Confianza S.A (en adelante la Aseguradora) es establecer el marco general para proteger los activos de información de la organización, asegurando su confidencialidad, integridad, disponibilidad y trazabilidad, de acuerdo con los requerimientos legales, regulatorios y del negocio.

La política orienta todas las actividades relacionadas con la gestión, el uso y la protección de la información, promoviendo una cultura de seguridad entre los colaboradores, contratistas y terceros, garantizando que la información sea utilizada de manera responsable, segura y alineada con los objetivos estratégicos de la compañía.

Principios orientadores:

- **Confidencialidad:** La información será accedida únicamente por personas autorizadas.
- **Integridad:** La información se mantendrá exacta, completa y sin alteraciones no autorizadas.
- **Disponibilidad:** La información estará disponible para quienes la requieran en el momento oportuno.
- **Legalidad:** Se cumplirá con las leyes y normativas vigentes en materia de protección de datos y seguridad.
- **Responsabilidad compartida:** Todos los colaboradores son responsables de proteger la información y reportar incidentes.
- **Mejora continua:** Se promoverá la revisión, actualización y fortalecimiento constante del Sistema de Gestión de Seguridad de la Información (SGSI).

2 DESCRIPCIÓN DE LAS POLÍTICAS

Esta política se debe leer junto con los siguientes Manuales:

Sistema de Gestión de Seguridad de la Información - SGSI GR-MA-37-**.

Manual gestión antivirus GR-MA-12-**.

1. POLÍTICA DE SEGURIDAD y CIBERSEGURIDAD

Política de Seguridad de la Información

Seguros Confianza S.A gestionará la Seguridad de la Información y la Ciberseguridad en todos los procesos de la organización, garantizando la protección de sus activos de información mediante la preservación de su confidencialidad, integridad y disponibilidad, así como de cualquier otra propiedad requerida para asegurar su adecuada gestión.

La Aseguradora implementará esta política a través de un Sistema de Gestión de Seguridad de la Información (SGSI), soportado en:

- Una gestión de riesgos integral,

- Un equipo humano capacitado y consciente de sus responsabilidades, y
- Una infraestructura tecnológica adecuada y segura.

Seguros Confianza S.A. se compromete a establecer, mantener y mejorar continuamente medidas y controles que permitan prevenir, detectar, responder y recuperarse ante incidentes de Seguridad de la Información, garantizando el cumplimiento de los requisitos regulatorios, contractuales y corporativos aplicables.

1.1.1 Revisión de la Política

Anualmente en la Junta Directiva se revisará la política para garantizar su cumplimiento y su adecuada gestión de acuerdo con los objetivos del negocio.

Políticas Generales:
Seguros Confianza S.A establece las siguientes políticas generales de Seguridad de la Información y Ciberseguridad, las cuales se alinean con el tratamiento y protección de los activos de Información de la Aseguradora:

- La Junta Directiva será el responsable de la revisión y mejora de la Política de Seguridad de la Información y Ciberseguridad.
- Los Activos de Información, serán identificados y clasificados por el área de riesgos para establecer e implementar los controles necesarios para mitigar los riesgos asociados a cada uno de ellos.
- Se realizarán auditorías y revisiones periódicas sobre la Política de Seguridad de la Información.
- Es responsabilidad de todos los colaboradores reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que ocurran.
- Las violaciones a las políticas y controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.
- La Aseguradora contará con un Plan de Continuidad del Negocio que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos relacionados con Seguridad de Información y Ciberseguridad.

Adicionalmente Seguros Confianza S.A cuenta con políticas específicas del negocio, un conjunto de estándares TI y procedimientos que soportan la Política de Seguridad de la Información.

2. POLÍTICAS Y PROCEDIMIENTOS PARA EL INTERCAMBIO DE INFORMACIÓN

Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información a través del uso de todo tipo de servicios de comunicación.

3. POLÍTICAS PARA EL CONTROL DE ACCESO

- Es responsabilidad de la Gerencia de Gestión Humana informar oportunamente la contratación, retiro o ausencia por vacaciones, incapacidad o licencias de personal con el cual se procede a hacer la adecuada gestión de las cuentas de usuario.

- Los privilegios y permisos de acceso a los sistemas de información de Seguros Confianza S.A serán creados con base a los roles y perfiles definidos en la matriz de accesos.

- Los privilegios y permisos de acceso a los sistemas de información serán eliminados o restringidos en caso de retiro, vacaciones, incapacidad o licencias.

- El Director de Seguridad de la Información es responsable de autorizar la creación, eliminación o desactivación de cuentas de usuario debido a contratación, retiro, vacaciones, incapacidad o licencias, informadas por recursos humanos. Así mismo hará seguimiento del cumplimiento de la política los dos (2) días hábiles siguientes de notificada la novedad.

- El Director de Seguridad de la Información es responsable de hacer seguimiento y monitoreo de las cuentas en los sistemas de información de la Aseguradora con base al reporte de novedades y ausencias enviado por la Gerencia de Gestión Humana esta revisión se hará cada cuatro (4) meses.

- Las cuentas de los servicios de los sistemas de información se encuentran en el documento inventario de usuarios administradores, y hacen parte de una gestión especial de contraseñas ya que la expiración de estas cuentas puede causar una caída en los servicios y sistemas de información de la Aseguradora.

- Las cuentas de usuario que se encuentren creadas y nunca han sido utilizadas se eliminaran de los sistemas de información de la Aseguradora.

- Las cuentas que usuario del directorio activo que no han sido utilizadas en los últimos cuarenta y cinco (45) días calendario serán deshabilitadas.

- La creación de cuentas de usuario será informada por el Director de Seguridad de la Información a los nuevos usuarios una vez hayan sido enviadas por los administradores de los diferentes sistemas de información de la Aseguradora.

- Las cuentas de usuario que se encuentren creadas y haya pasado dos (2) meses sin haber sido utilizadas se investigara lo sucedido con el usuario y se eliminaran de los sistemas de información de la Aseguradora si no se van a seguir utilizando.

- Para la Eliminación o desactivación de usuarios en:

Osiris: En caso de retiro, vacaciones, incapacidad o licencias solo se desactiva el usuario esto en el fin de proteger la integridad de la base de datos del aplicativo.

Directorio Activo: En caso de retiro se eliminará la cuenta del usuario del directorio activo. En caso de vacaciones, incapacidad o licencias, se desactivará las cuentas de acuerdo con el tiempo de ausencia.

- Se crea el Procedimiento: Gestión de Cuentas de Usuario y Acceso a Plataforma tecnológica. Este Procedimiento define desde el inicio de la vinculación de un colaborador de la Aseguradora, la asignación de los permisos y privilegios que posee, y revocación de estos.

4. POLÍTICA DE CREACIÓN DE CONTRASEÑAS DE USUARIO

Es responsabilidad de los colaboradores de la Aseguradora la creación de contraseñas robustas en materia de Seguridad. Para esto se deben seguir los siguientes lineamientos:

- ✓ La contraseña debe tener una longitud mínima de ocho (8) caracteres.
- ✓ La contraseña debe ser una combinación de letras mayúsculas, minúsculas, números y caracteres especiales (&, %, $, #, @, +,etc).
- ✓ La contraseña no debe estar conformada por nombres, palabras conocidas o palabras asociadas a su vida personal (ej: nombre de hijo, esposo, mascota, fecha de nacimiento, número de teléfono, cédula de identidad, etc.).
- ✓ Esta prohibido escribir las contraseñas en cualquier lugar donde alguna persona pueda visualizarla fácilmente, lo recomendable es memorizarla.
- ✓ La contraseña se debe cambiar cada sesenta (60) días.
- ✓ Está prohibido asignar las últimas veinte (20) contraseñas utilizadas.
- ✓ En caso de bloqueo por intentos fallidos se debe solicitar a la mesa de ayuda el cambio de esta.
- ✓ El usuario debe cambiar su contraseña inmediatamente después de su primer uso y/o al solicitar un cambio por olvido o bloqueo.

5. POLÍTICA DE ESCRITORIO Y PANTALLA DESPEJADOS.

- Es responsabilidad de los Colaboradores:
  - ✓ No dejar a la vista documentos sensibles en el escritorio.
  - ✓ Bloquear la estación de trabajo al alejarse del puesto.
  - ✓ No escribir contraseñas u otros datos sensibles en papeles a la vista.
  - ✓ Dejar bajo llave equipos y documentos.
  - ✓ Asegurar con candados estaciones de trabajo portátiles.
  - ✓ Tener precaución con la información que se muestra en la pantalla de la estación de trabajo cuando hay visitas en la oficina.
  - ✓ Dedicar algunos minutos a guardar documentos y otros elementos de cuidado.
  - ✓ Cerrar con llave los cajones.
  - ✓ Cuidar de no dejar tableros con información sensible.

6. POLÍTICA DE USO DE LOS SERVICIOS EN RED

Los usuarios sólo poseen acceso a los servicios asignados a través de su usuario del directorio activo, a cuyo uso están específicamente autorizados.

7. POLÍTICA DE GESTIÓN DE CONTRASEÑAS PARA LOS SISTEMAS DE INFORMACIÓN

La Gerencia de Tecnología es responsable de la implementación de las políticas de contraseña de usuarios aplicadas a las cuentas del directorio activo para esto se seguirán las mejores prácticas en seguridad que se describen a continuación:

- ✓ Histórico de contraseñas (veinte (20) contraseñas recordadas)
- ✓ Máxima vigencia contraseña (sesenta (60) días)
- ✓ Mínima vigencia de contraseña (dos (2) días)
- ✓ Longitud de contraseña (catorce (14) caracteres mínimo)
- ✓ Requerimientos de complejidad (activado)
- ✓ Duración del bloqueo de cuentas (cero (0) minutos la cuenta permanecerá bloqueada hasta que se solicite el desbloque a la mesa de ayuda)
- ✓ Bloqueo de cuentas por error de contraseñas (tres (3) intentos incorrectos)
- ✓ Resetear las contraseñas (sesenta (60) minutos)
- ✓ El usuario debe cambiar su contraseña inmediatamente después de su primer uso y/o al solicitar un cambio por olvido o bloqueo.

- ➢ Es Responsabilidad de la Gerencia de Tecnología hacer la parametrización y la implementación de las políticas de contraseña de usuarios aplicadas a las cuentas de usuario de Osiris para esto se seguirán las mejores prácticas en seguridad que se describen a continuación:

  - ✓ Histórico de contraseñas (veinte (20) contraseñas recordadas)
  - ✓ Máxima vigencia contraseña (sesenta (60) días)
  - ✓ Mínima vigencia de contraseña (dos (2) días)
  - ✓ Longitud de contraseña (ocho (8) caracteres mínimo)
  - ✓ Requerimientos de complejidad (activado)
  - ✓ Duración del bloqueo de cuentas (cero (0) minutos la cuenta permanecerá bloqueada hasta que el administrador de Osiris lo desbloquee)
  - ✓ Bloqueo de cuentas por error de contraseñas (tres (3) intentos incorrectos)
  - ✓ Reiniciar las contraseñas (sesenta (60) minutos)
  - ✓ El usuario debe cambiar su contraseña inmediatamente después de su primer uso y/o al solicitar un cambio por olvido o bloqueo.

- ➢ Las mejores prácticas en seguridad que se mencionaron anteriormente aplican para todos los sistemas de información de la compañía.

7. POLÍTICA DE CONTRASEÑAS PARA LA ADQUISICIÓN DE NUEVOS EQUIPOS:

- Es Responsabilidad de la Gerencia de Tecnología cambiar las contraseñas por defecto proporcionadas por fabricantes debido al ingreso de nueva infraestructura tecnológica y dispositivos de comunicaciones en el ambiente de producción.

8. POLÍTICA DE NEMOTÉCNICA DE EQUIPOS:

La Gerencia de Tecnología es responsable del nombramiento de los servidores y estaciones de trabajo de la Aseguradora, estos se escribirán en mayúsculas.

- Se utilizará la mitología griega para nombrar los servidores de la organización. Si varios servidores ofrecen el mismo servicio se creará un numero con el mismo nombre por ejemplo puede existir:
- ZEUS, ZEUS I, ZEUS II
- Para las estaciones de trabajo se utilizará la siguiente nomenclatura:
- XXXCONFIYYY
- En el cual XXX representa el número identificador de la sucursal, YYY representa el consecutivo asignado al equipo.

9. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de la información.

2.1.1 ACCIONES ESTRATÉGICAS PARA EL DESARROLLO DE LA POLÍTICA

Para garantizar la implementación, efectividad y mejora continua de esta política, la Aseguradora adopta las siguientes acciones estratégicas:

- **Gobernanza y liderazgo:**
  - ✓ Mantener informada a la Junta Directiva como órgano rector del SGSI.
  - ✓ Asignar responsabilidades claras en materia de seguridad de la información a todos los niveles de la organización.
- **Gestión de riesgos:**
  - ✓ Identificar, evaluar y tratar los riesgos asociados a los activos de información mediante una metodología formal y periódica.
  - ✓ Mantener actualizado el inventario de activos de información y su clasificación.
- **Capacitación y cultura organizacional:**
  - ✓ Desarrollar programas continuos de sensibilización y formación en Seguridad de la Información.
  - ✓ Fomentar la cultura del reporte oportuno de incidentes y eventos de seguridad.
- **Gestión tecnológica y de controles:**
  - ✓ Implementar medidas técnicas y administrativas que garanticen la protección de los sistemas y servicios críticos.
  - ✓ Aplicar políticas de contraseñas, control de accesos, criptografía, uso de red y continuidad del negocio según las mejores prácticas.

- **Cumplimiento y auditoría:**
  - ✓ Realizar revisiones periódicas y auditorías internas del SGSI para verificar la eficacia de los controles.
  - ✓ Garantizar la conformidad con los requisitos legales, regulatorios y contractuales aplicables.

- **Mejora continua:**
  - ✓ Revisar la política anualmente y actualizarla conforme a los cambios tecnológicos, normativos y de negocio.
  - ✓ Incorporar las lecciones aprendidas de incidentes, auditorías y revisiones de desempeño.

CONTROL DE CAMBIOS

VERSIÓN	FECHA	ELABORADO POR	APROBADO POR	BREVE DESCRIPCIÓN DEL CAMBIO
01	02-02-2024	Dollceys Mestre- Director de seguridad de la información y gobierno de datos	Junta Directiva Febrero 2024 (acta No 593)	*Se crea documento de Política de Seguridad da la información. Esta información se encontraba inmersa en el Manual Interno de Seguridad de la Información. *Se crea la codificación GR-PL-05-01
02	26-02-2026	Dollceys Mestre- Director de seguridad de la información y gobierno de datos Wbeimar Marín- Gerente de riesgo	Junta Directiva (acta No 620)	*Se realizan ajustes de forma para un mejor entendimiento de la Política *Se presentó para ratificación por parte de la Junta Directiva.