POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Vicepresidencia de Tecnología
Gerencia de Ciberseguridad

“Este documento está disponible en los sistemas oficiales para publicar cuya versión siempre será la última revisada y aprobada. Las copias físicas son consideradas no controladas”

Este documento es de uso público

Contenido

1. OBJETIVO

Establecer y dar a conocer las directrices, lineamientos, practicas, procesos y procedimientos aplicables para la utilización segura de los activos de información para todo el personal directo, temporal, pasantes, practicantes, outsourcing, terceros, proveedores, consultores, contratistas, socios de negocio, clientes y demás partes interesadas con acceso a activos de información de HDI Seguros. El Sistema de Gestión de Seguridad de la Información (SGSI) incluye un componente para aumentar periódicamente el grado de conciencia, capacitación y educación de los usuarios acerca de sus responsabilidades de seguridad de la información para mantener la confidencialidad, integridad, disponibilidad y protección de la privacidad de esta. Adicional se tendrán en cuenta las leyes vigentes aplicables para asegurar el cumplimiento de los requisitos regulatorios y contractuales derivados de las obligaciones adquiridas por relaciones comerciales.

2. ALCANCE

La Política de Seguridad de la Información y ciberseguridad aplica para:

- Todos los colaboradores y no colaboradores que trabajan para o en representación de HDI Seguros; incluyendo personal directo, temporal, pasantes, practicantes, outsourcing y consultores (denominados en forma conjunta el "Personal");
- Todos los contratistas, terceros, proveedores y socios que acceden y usan nuestros datos, sistemas informáticos y/o redes;
- Demas partes interesadas que apliquen.
- Todos los activos de información/datos, sistemas de procesamiento de información/computadoras y redes (incluyendo computación basada en la nube, ambientes denominados en forma conjunta como los "activos de información") pertenecientes a/o que estén bajo el control de HDI Seguros.
- Todo el ciclo de vida de la información (generación, distribución, procesamiento, almacenamiento, consulta y destrucción).

Esta política, junto con los estándares que la soportan, establecen el marco de seguridad para la información de propiedad o controlada por HDI Seguros. Las declaraciones de políticas en este documento están soportadas por una serie de procedimientos operativos documentados, controles técnicos embebidos en los sistemas de información y otros controles recomendados y recordados al personal de manera regular.

3. MARCO LEGAL / NORMATIVO

3.1. Externo:

- **ISO/IEC 27001:2022**: Norma ISO "Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de seguridad de la información - Requisitos" que incorpora el enfoque de "planificar-hacer-verificar-actuar" de Deming para la mejora continua.

- **ISO/IEC 27002:2022**: Guía ISO "Seguridad de la información, ciberseguridad y protección de la privacidad – controles de seguridad de la información". Contiene un conjunto completo de objetivos de control de seguridad de la información y una selección de controles de seguridad de la información de mejores prácticas.
- **ISO/IEC 27005: 2022**: Proporciona directrices fundamentales para la gestión de riesgos de seguridad de la información en la identificación, análisis, evaluación y tratamiento de riesgos, ayudando a proteger activos y mejorar la resiliencia.
- **ISO/IEC 42001:2023**: Es la norma internacional para sistemas de gestión de la inteligencia artificial (IA), el cual define como una organización debe diseñar, usar y gobernar la IA de forma responsable.
- **Ley 1273 de 2009**: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1581 de 2012**: Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.
- **Ley 1266 de 2008**: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 23 de 1982**: Leysobre los derechos de autor.
- **Ley 1074 de 2015**: Capitulo 25 Reglamentar parcialmente la ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales y Capitulo 26 Reglamentar la información mínima que debe contener el Registro Nacional de bases de datos, creado por la ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los responsables del tratamiento.
- **CONPES 3975 de 2024**: Formula una política nacional para la transformación digital e inteligencia artificial. Esta política tiene como objetivo potenciar la generación de valor social y económico en el país a través del uso estratégico de tecnologías digitales en el sector público y el sector privado, para impulsar la productividad y favorecer el bienestar de los ciudadanos, así como generar los habilitadores transversales para la transformación digital sectorial, de manera que Colombia pueda aprovechar las oportunidades y enfrentar los retos relacionados con la Cuarta Revolución Industrial (4RI).
- **Decreto 1377 de 2013**: Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.
- **Circular Externa 002 de 2024 de la Superintendencia de Industria y Comercio de Colombia:** Lineamientos sobre el Tratamiento de datos personales en sistemas de Inteligencia Artificial.
- **Circular Externa 033 de 2020 de la Superintendencia Financiera de Colombia**: la Superintendencia Financiera imparte instrucciones relacionadas con la Taxonomía Única de Incidentes Cibernéticos –

TUIC, el formato para el reporte de métricas de seguridad de la información y ciberseguridad y el protocolo de etiquetado para el intercambio de información Traffic Light Protocol, TLP.

- **Circular Externa 007 de 2018 la Superintendencia Financiera de Colombia:** Imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad.
- **Circular Externa 006 de 2025** Capítulo V "Requerimientos mínimos para la gestión del riesgo de ciberseguridad" del Título IV de la Parte I.
- **Circular Externa 005 de 2019 de la Superintendencia Financiera de Colombia**: Imparte instrucciones reglas relativas al uso de servicios de computación en la nube.
- **Reglamento 2024/1689, Unión Europea:** AI ACT. Adopta un enfoque basado en riesgo para garantizar la seguridad y los derechos fundamentales en el uso de la IA. También crea un marco de gobernanza con autoridades nacionales y se crea la Junta Europea de IA (EAIB).
- Las guías proporcionadas por Talanx en Alemania como casa matriz de la operación de HDI Seguros Colombia.
- Demas tratados y acuerdos que hagan referencia a la seguridad de la información y privacidad de datos que nos apliquen y sirvan como referencia para garantizar la confidencialidad, integridad y disponibilidad de la información de HDI Seguros.

3.2. Interno:

- **Código de ética**: Se detallan los valores, principios y lineamientos éticos bajo los que opera HDI Seguros.
- **Reglamento interno de trabajo**: Establece los derechos y obligaciones de los colaboradores que tienen una relación contractual de trabajo con HDI Seguros.
- **Cláusulas contractuales**: Para las partes interesadas que apliquen se deberán establecer cláusulas que describen las responsabilidades de las partes frente a la seguridad de la información y ciberseguridad y protección de datos. Así como las sanciones frente a su incumplimiento.
- **Política de Tratamiento de datos personales**: Establece los lineamientos sobre el tratamiento de datos impartidos desde la compañía.

4. GOBIERNO:

4.1. Modelo de las tres líneas de defensa

La adecuada rendición de cuentas para la gestión del riesgo operacional es esencial. La estructura de "tres líneas de defensa" es una de las formas de lograr ese objetivo. A continuación, los roles y responsabilidades de cada una:

- **Primera línea**

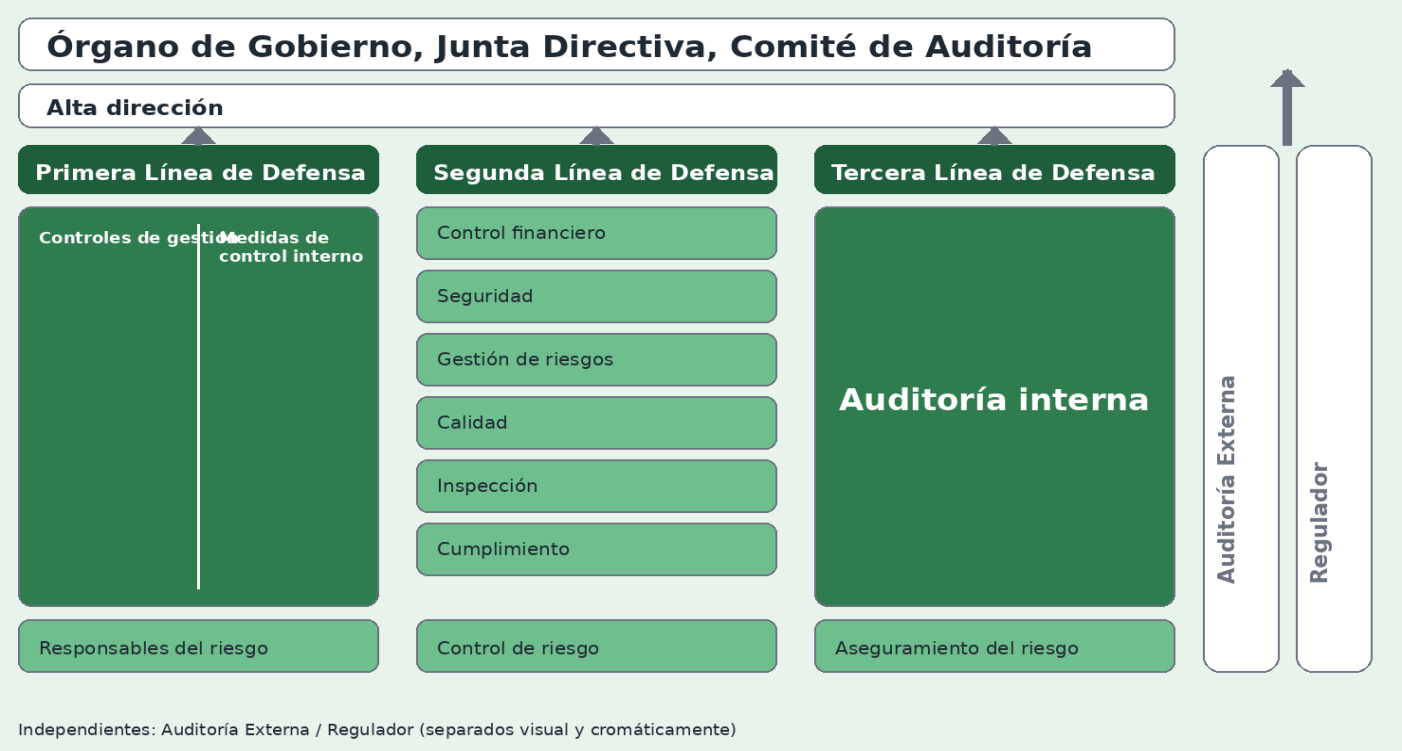
Los propietarios de los procesos de gestión y control serán responsables de mantener controles internos eficaces y de ejecutar los procedimientos de gestión de riesgos y control diariamente.

- **Segunda línea**

La segunda línea proporciona orientación sobre cumplimiento normativo y gestión de riesgos para la identificación de riesgos emergentes en la operación diaria y programas de pruebas de control para demostrar la supervisión de la gestión del funcionamiento de los controles.

- **La tercera línea**

La tercera línea, son los auditores internos, proporciona al órgano de gobierno y a la alta dirección una garantía basada en el riesgo, con el máximo nivel de independencia y objetividad dentro de la organización.



Fuente: Imagen adaptada de la página de PricewaterhouseCoopers (PWC) Colombia febrero 03, 2026

4.2. Junta Directiva: Tiene como responsabilidad principal dentro del Sistema de Gestión de Seguridad de la Información (SGSI) la aprobación de la estrategia de seguridad de la información y ciberseguridad.

4.3. La Alta Gerencia: La alta gerencia es responsable de dar buen ejemplo a los colaboradores tomando el liderazgo en la promoción de los procesos de concientización en seguridad de la información y aplicando buenos principios en su trabajo.

4.4. Comité de Seguridad de la Información: Toma de decisiones de acuerdo con su alcance, incorporación de medidas de mitigación de riesgos de seguridad de la información y hacer cumplir los lineamientos de las políticas.

4.5. Vicepresidencia de Tecnología: La Vicepresidencia de Tecnología es responsable de asegurar que las políticas de seguridad de la información, estándares y procedimientos sean implementadas en aplicaciones, sistemas de información e infraestructura.

4.6. Gerente de Ciberseguridad: Entre varias de sus responsabilidades, la principal corresponde a administración del Sistema de Gestión de Seguridad de la Información. Está autorizado por la Junta Directiva para tomar las medidas necesarias para establecer, implementar y administrar el Programa de Seguridad de la Información.

4.7. Director de Gobierno / Sistema de Gestión de Seguridad de la Información (SGSI): Es el responsable de aplicar y soportar una adecuada gestión de Seguridad de la Información y Ciberseguridad con el fin de proteger la información de la compañía, preservando la confidencialidad, integridad, disponibilidad y la protección de la privacidad de la información.

4.8. Director de Seguridad, Aplicaciones y Cloud: Es el responsable de la protección de los activos digitales, garantizando que las aplicaciones y servicios obtenidas y/o desarrolladas en la nube, estén seguros y cumplan con las normativas de privacidad y estándares de seguridad que le apliquen, igualmente debe gestionar un adecuado entorno cloud guiado por los lineamientos de seguridad de la información.

4.9. Ingenieros / Analistas y Consultores de Seguridad de la información y Ciberseguridad: Son responsables en el apoyo al cumplimiento de las políticas de Seguridad de la información y ciberseguridad, estándares y procedimientos, así como del monitoreo de su cumplimiento.

4.10. Gerente de Legal: En su calidad de asesor en el cumplimiento de normativas y regulaciones locales en materia de seguridad de la información y ciberseguridad, así como en temas de confidencialidad y privacidad en los contratos**.**

4.11. Gerente de Cumplimiento: En su calidad de apoyo a la Vicepresidencia de Tecnología en los riesgos derivados de la conservación de registros y protección y privacidad de datos personales de las partes interesadas**.**

4.12. Centro de Operaciones de Seguridad (SOC): El centro de operaciones de seguridad (SOC) es el encargado de ejecutar las siguientes tareas: Monitorear, prevenir, detectar, investigar y alertar las amenazas de ciberseguridad. El personal designado debe estar disponible las 24 horas del día, los 7 días de la semana para responder a incidentes de seguridad que le apliquen. Brindar respuesta al área de ciberseguridad en caso de un incidente. Investigar excepciones y anomalías identificadas durante el proceso de revisión de registros.

4.13. Clientes y Socios de Negocios: Los clientes y socios de negocio deberán ejercer el debido cuidado y precaución cuando tengan acceso a los sistemas y activos de información de HDI Seguros; esto incluye asegurar que la confidencialidad, integridad, privacidad y la protección de la privacidad, de la información es salvaguardada de manera adecuada.

4.14. Proveedores: Los proveedores deberán cumplir con los acuerdos contractuales establecidos con HDI Seguros y cumplir con las políticas y procedimientos establecidos al interior de la compañía.

4.15. Colaboradores: Todo el personal, de acuerdo con lo establecido en el alcance, que crea, recibe, o controla, en todas sus formas, electrónica y física, información de la compañía tiene la obligación de salvaguardarla y protegerla. Todos son responsables de revisar, entender y cumplir con esta Política y los estándares aplicables a su función de trabajo que la soportan. Adicionalmente están obligados a notificar a través de los medios establecidos e implementados acerca de cualquier incidente o problema de seguridad conocido o sospechado.

4.16. Vicepresidencia de Talento y Cultura: Es el responsable de emitir y supervisar los lineamientos con relación a los derechos, deberes y obligaciones de las personas que hacen parte de la compañía.

5. DESCRIPCIÓN DE LA POLÍTICA

La siguiente política de seguridad de la información está bajo la referencia de las normas ISO/IEC 27001, y la guía ISO/IEC 27002, en sus versiones actualizadas y se alinean con los objetivos de control de este estándar. Este documento de Política de Seguridad de la Información y Ciberseguridad provee un marco de trabajo para garantizar que la confidencialidad, integridad, disponibilidad y la protección de la privacidad, de la información, con el cual se mantiene y mejora continuamente, se gestionan las amenazas y las vulnerabilidades y los riesgos de seguridad de la información, ciberseguridad y protección de la privacidad.

5.1. Jerarquía de la Política de Seguridad de la Información y ciberseguridad

Esta Política de Seguridad de la Información y ciberseguridad define las capas de la jerarquía de la política de seguridad de la información de HDI:

- **Los principios rectores**: Son objetivos de control amplios y generales para la seguridad de la información que brindan estrategias a la dirección de seguridad de la información.
- **Las políticas**: Son directrices específicas de la Gerencia de Ciberseguridad, existen numerosas políticas dentro del Sistema de Gestión de Seguridad de la Información (SGSI), que se relacionan directamente con los objetivos de control que figuran en la norma ISO/IEC 27002. Los objetivos de control definen el porqué de la seguridad de la información es importante para HDI Seguros.
- **Los estándares**: Proporcionan un detalle sobre los controles de seguridad de la información y explican cómo las directrices de la política deben ser integradas en las plataformas de sistemas.

- **Los procedimientos de seguridad de la información**: Se encuentran documentados y definen controles para la gestión de la seguridad con el fin de cumplir con las políticas.
- **Las Directrices**: ofrecen más información y consejos útiles sobre seguridad de la información a los usuarios de los activos de información de HDI Seguros. A pesar del nombre, las directrices incluyen una mezcla de controles obligatorios relativos a los estándares de más alto nivel, las políticas y los principios, así como los controles opcionales e información de apoyo para ayudar al personal a entender y aplicar la seguridad de la información de manera eficiente.

5.2. Principios Guía de la Seguridad de la Información y ciberseguridad

A continuación, se presentan siete Principios fundamentales de seguridad de la información que respaldan en su totalidad la jerarquía de la política en HDI Seguros:

- **Principio 1 - Cumplimiento de Normas**: Nuestro sistema de seguridad de la información, sigue las reglas y mejores prácticas internacionales para proteger la información.
- **Principio 2 - Protección de Información**: La información es muy valiosa para nosotros y debemos protegerla adecuadamente.
- **Principio 3 - Controles de Seguridad**: Establecemos medidas para proteger la información contra riesgos como la divulgación no autorizada, errores y fallos, y tiempos de inactividad.
- **Principio 4 - Inversión Inteligente**: Invertimos en medidas de seguridad cuando es necesario, buscando siempre el equilibrio entre costo y beneficio.
- **Principio 5 - Responsabilidad Compartida**: La seguridad de la información es responsabilidad de todos en HDI Seguros y está integrada en nuestros procesos y sistemas.
- **Principio 6 - Gobierno Corporativo**: La seguridad de la información es parte de la gestión de la compañía y está relacionada con la seguridad física, la gestión de riesgos, el cumplimiento legal y la continuidad del negocio.

- **Principio 7 - Habilitador de Negocios**: La seguridad de la información nos permite mantener relaciones de negocios con confianza y entrar en nuevos mercados, apoyando nuestros resultados financieros y mejorando nuestra imagen corporativa

6. LINEAMIENTOS

6.1. Gestión del cumplimiento de las Políticas De Seguridad y Ciberseguridad

Esta Política, junto con los estándares de apoyo, establece procesos y procedimientos obligatorios. Cada usuario de la información y los sistemas de HDI Seguros es y será responsable de cumplir con esta Política. El incumplimiento puede exponer a HDI Seguros y sus partes interesadas a riesgos innecesarios y puede comprometer los activos de información. Las violaciones de esta Política pueden resultar en una acción disciplinaria, sanción administrativa e incluso legales.

Riesgo Operativo y la Gerencia de Ciberseguridad son responsables de realizar revisiones periódicas para asegurar el cumplimiento de esta Política.

Nivel de la falta	Descripción de la falta
Leve	Error que no compromete a los activos de la información de la compañía.
Moderado	Incumplimiento de los lineamentos establecidos en el sistema de forma consciente y como consecuencia pueden provocar un incidente de seguridad que comprometa a algún activo de la información.
Grave	Incumplimiento de los lineamentos establecidos en el sistema por acciones deliberadas con el fin de ocasionar daño o un beneficio propio y como consecuencia compromete alguno de los activos de la información.

Para promover la participación de la Alta Dirección con respecto al Sistema de Gestión de Seguridad de la Información (SGSI) la Gerencia de Ciberseguridad conforma el Comité de Seguridad de la Información quienes, de manera transversal velaran por el cumplimiento y comunicaran los lineamientos de la presente Política.

El Gerente de Ciberseguridad es responsable de mantener esta política, teniendo en cuenta, los siguiente:

- Cambios en los principios y políticas.
- Cambios en el entorno comercial o la estrategia corporativa (por ejemplo, nuevas prioridades comerciales, fusiones o enajenaciones, cambios en la estructura de HDI Seguros o en la jerarquía administrativa).
- Cambios en el entorno de riesgo de ciberseguridad (es decir, cambios en las vulnerabilidades, amenazas o impactos de ciberseguridad y tendencias emergentes).
- Obligaciones legales y reglamentarias nuevas o modificadas que afectan el procesamiento de la información y el gobierno de TI.

- Avances en las mejores prácticas de seguridad y asesoramiento sólido de cualquier fuente, incluidas las revisiones de los estándares de seguridad cibernética pertinentes.
- La frecuencia de revisión y actualización dependerá de las situaciones mencionadas anteriormente y en todo caso no excederá de 1 año para su revisión.

6.2. Gestión del cumplimiento de los requisitos normativos, legales y contractuales

Como parte de las estrategias establecidas para HDI Seguros y para entregar confianza a nuestras partes interesadas, se implementan no solo los requerimientos de la norma ISO/IEC 27001:2022 sino que además contribuimos con el cumplimiento de los requisitos legales y contractuales relevantes para la compañía.

Como objetivo principal HDI Seguros deberá cumplir con las normas aplicables al Sistema, las cuales se identifican en la "Matriz de requisitos legales de la compañía", dando prioridad a la privacidad y protección de datos personales.

Sin embargo, no se deberá dejar de lado toda la información de la organización, sin distinción de que contenga datos personales o no, garantizando su confidencialidad, integridad, disponibilidad y la protección de la privacidad.

6.3. Gestión de los activos de información y su clasificación

La información de la compañía debe tener asignado un propietario que sea responsable de la gestión adecuada de la misma. Los propietarios de los Activos de Información tienen la responsabilidad principal sobre los procesos de negocio a través de los cuales se recibe, crea, almacena, manipula o descarta la información, ya sea en forma física o electrónica.

Los propietarios de activos de información son responsables de la autorización de acceso a la información por parte de los usuarios, el control de cambios en la información y por asegurar que las funciones y aplicaciones esenciales de negocio sean recuperables en el caso de que el entorno existente no esté disponible.

La información de la compañía debe clasificarse de acuerdo con lo siguiente:

- **Restringido:** Información que es extremadamente sensible y/o crítica para el negocio y, por lo tanto, debe protegerse lo más posible contra el acceso no autorizado. Los ejemplos incluyen estrategias, planes, actas de la Junta, minutas del comité de seguridad de información, documentación organizacional del sistema, informes anuales de HDI Seguros antes de su publicación, contraseñas, reglas de firewall, entre otras.
- **Confidencial:** Información que es sensible y/o crítica para el negocio y, por lo tanto, debe protegerse en una medida razonable. Está destinado a una distribución limitada dentro de HDI Seguros o a

terceros especialmente designados, en función de la necesidad de conocer (por ejemplo, información financiera de clientes, evaluaciones de riesgos, procedimientos).

- **Uso Interno:** Información destinada al uso general del personal de HDI Seguros y, si es necesario, de terceros seleccionados, como clientes, proveedores o contratistas (por ejemplo, políticas de la Compañía y presentaciones de los departamentos).
- **Pública:** Información que ha sido clasificada oficialmente por HDI Seguros, para publicación externa a grupos específicos o al público en general (por ejemplo, comunicados de prensa, materiales de marketing) o que ya es de dominio público (por ejemplo, periódicos, sitios web públicos de Internet).

Con relación a la clasificación de información, esta deberá ser etiquetada para su fácil y rápida identificación.

El intercambio de información deberá contar con los siguientes requisitos.

- Se contará con la previa autorización del propietario del activo de información.
- Se realizará por canales corporativos autorizados y la seguridad de estos alineada la "Política de gestión de cifrado".
- Se contará con mecanismos automáticos que permitan la protección de la información a intercambiar.
- Se contarán con mecanismos automáticos de detección de la información en los activos.
- Se controlará adicionalmente por medio de cláusulas contractuales que le apliquen.
- En caso de duda frente al tratamiento de la información a intercambiar, podrá consultar a las áreas de Ciberseguridad y/o Cumplimiento.

El tratamiento de la información deberá contar con los requisitos de seguridad establecidos en todo su ciclo, en caso de que se requiera obtener conocimiento sobre estas actividades, se cuentan con canales corporativos como el correo o medio de comunicación interna para solicitar indicaciones desde la parte técnica o legal.

6.4. Gestión del riesgo de seguridad de la información

La gestión del riesgo de seguridad de la información tiene por objetivo identificar las vulnerabilidades y amenazas, medir su impacto, y probabilidad de pérdida operativa, tecnológica, cuantitativa y establecer planes de tratamiento sobre los riesgos guiados por la norma ISO/IEC 27002:2022 Guía de "Seguridad de la información, ciberseguridad y protección de la privacidad – controles de seguridad de la información". El cual contiene un conjunto completo de objetivos de control de seguridad de la información y una selección de controles de seguridad de la información de mejores prácticas. Estas deben seguir la metodología de cuantificación de riesgo definida por el área de Riesgo Operativo.

La Gerencia de Ciberseguridad será la encargada de gestionar el riesgo de seguridad de la información que pueda poner en riesgo la confidencialidad, integridad, disponibilidad y la protección de la privacidad de la

información, priorizando las actividades críticas que puedan no solo afectar el sistema si no los objetivos estratégicos de HDI Seguros.

La gestión del riesgo contara con una matriz, una política, procedimiento y una metodología definida que permita establecer todos los aspectos para el análisis del riesgo, así como su periodicidad, la cual inicialmente será anual, cuando ocurra un cambio significativo o se presente un evento o incidente que amerite la evaluación del riesgo.

6.5. Gestión de Programa de seguridad y ciberseguridad

HDI Seguros cuenta con un programa de seguridad y ciberseguridad de la información para gestionar adecuadamente los riesgos de seguridad y proteger sus activos de información manteniendo la confidencialidad, integridad, disponibilidad y protección de la privacidad, así como de conservar la reputación y la marca de la compañía, evitando riesgos y soportando directamente los objetivos del negocio. Esto se logra a través de la política de seguridad de la información que deben cumplir todos los relacionados en el alcance.

HDI Seguros reconoce que tiene el deber de proteger la información. El programa de seguridad de la información y ciberseguridad debe identificar controles adecuados que procuren por la confidencialidad, integridad, disponibilidad y protección de la privacidad de la información y que se encuentra en el ciberespacio de acuerdo con las leyes, prácticas de negocio y estándares de la industria.

Con el objetivo de identificar los riesgos se analiza la naturaleza del ciberespacio y la ciberseguridad

- **Naturaleza del Ciberespacio:** El ciberespacio puede describirse como un entorno virtual, que no existe en ninguna forma física, sino en un entorno complejo o espacio resultante de la aparición de Internet, más las personas, organizaciones, y actividades en todo tipo de dispositivos tecnológicos y redes conectadas a él.

- **Naturaleza de la Ciberseguridad:** Las partes interesadas en el Ciberespacio tienen que proteger sus propios activos, para que prevalezca la utilidad del Ciberespacio. Los requisitos se están expandiendo para que las personas y organizaciones estén preparadas para enfrentar los riesgos y desafíos de seguridad emergentes para prevenir y responder de manera efectiva al uso indebido y a las explotaciones criminales.

La seguridad cibernética se relaciona con las acciones que las partes interesadas deberían tomar para establecer y mantener la seguridad en el ciberespacio. La ciberseguridad se basa en la seguridad de la información, de las aplicaciones, de la red y de Internet; La ciberseguridad es una de las actividades necesarias para el CIIP (Protección de la infraestructura de la información crítica) y, al mismo tiempo, el CIIP contribuye

a las necesidades básicas de seguridad (es decir, seguridad, confiabilidad y disponibilidad de infraestructura crítica) para lograr los objetivos de ciberseguridad.

6.6. Gestión con entes de control, autoridades y grupos de interés

La gestión con entes de control, autoridades y grupos de interés tiene por objetivo dar cumplimiento a los requerimientos de las instituciones de control, siendo una prioridad para HDI Seguros.

Así como mantener contacto con las autoridades respectivas dependiendo de las situaciones que surjan de un incumplimiento que por su naturaleza debe ser informado y dar un tratamiento a través de los requisitos legales.

Adicional se debe mantener contacto con grupos de interés como, proveedores expertos en seguridad de la información, entes de control y autoridades en la materia, con el fin de mejorar el conocimiento acerca de buenas prácticas, actualizaciones y notificaciones de alarmas u ataques como forma de anticiparse y generar una reacción oportuna.

Como parte de la mejora al Sistema de Gestión de Seguridad de la Información (SGSI) se deberá contemplar las auditorias de mantenimiento, de vigilancia, de recertificación, Ethical Hacking y escaneo de vulnerabilidades, entre otras, que permitan obtener una visión objetiva e imparcial del rendimiento del sistema y cumplimiento de los objetivos de control que apliquen.

6.7. Gestión organizacional

6.7.1. Gestión sobre el tratamiento de la información

En concordancia con la Ley de protección de datos personales 1581 de 2012, desde HDI Seguros se contempla la seguridad de la información en todo su ciclo de tratamiento, con la finalidad de preservar su confidencialidad, integridad, disponibilidad y protección de la privacidad en el intercambio, transmisión, transferencia, resguardo y destrucción de datos, tanto de la compañía como las partes interesadas que apliquen.

Razón por la cual toda entrega y recepción de información se deberá realizar por medio de canales seguros y cifrado en los casos que aplique, indiferente del tipo de comunicación, sea física, electrónica y verbal. Para ello se han establecido políticas y procedimientos que contienen los pasos desde su autorización hasta su destrucción o resguardo.

6.7.2. Gestión de Identidades y Accesos (IAM)

La gestión de identidades y accesos tiene por objeto establecer lineamientos para el control adecuado de las identidades. Su función principal es la administración, aprobación, evaluación, protección y seguimiento de los roles y perfiles de los principales sistemas y aplicaciones Core de la compañía, aplicando el principio de ***mínimo privilegio*** con el fin de que cada cargo solo ejecute las funciones que le corresponden.

Como parte del monitoreo y control la Dirección de Gobierno de Seguridad de la Información, está a cargo de las revisiones anuales, realizando evaluaciones críticas y objetivas, obteniendo resultados que posteriormente serán informados a las Vicepresidencias, Auditoría Interna y Riego Operativo para que continue con los procesos correspondientes a nivel organizacional, pero fuera del sistema.

6.7.3. Gestión de accesos, usuarios y perfiles

HDI Seguros designara un equipo para realizar, las altas, modificaciones o bajas de usuarios de los aplicativos a su alcance en la organización, siempre asegurando una adecuada segregación de funciones, de acuerdo con los lineamientos de IAM y de Riesgo Operativo, limitado a usuarios plenamente identificados con la respectiva ***necesidad de conocer.***

Los lineamientos se establecen en detalle en la Política de ID management.

Para los demás equipos que asignen permisos de accesos en la compañía, rigen los mismos lineamentos antes indicados

6.7.4. Gestión de relación con proveedores

El objetivo principal es establecer relaciones seguras, perdurables y beneficiosas con terceros sin dejar de lado la protección de la información, por lo cual se hace necesario:

- Contar con un registro de proveedores y los servicios que prestan que será realizada por el área de abastecimiento.
- Establecer una clasificación de Riesgo Operativo, identificando proveedores críticos con el fin de fortalecer los controles a nivel contractual.
- Determinar las cláusulas contractuales de seguridad de la información y ciberseguridad, bajo las que operará y responderá en caso de incidentes de seguridad.
- Definir requisitos de seguridad de la información de acuerdo con el acceso al activo de la información y al servicio contratado por HDI Seguros.
- Proporcionar una adecuada gestión de cambio de servicios, en la que se pueda ver afectada la compañía.

- Se realizarán análisis periódicos, evaluaciones, así como auditorias como se determine conveniente, para detectar e incluir controles sobre cambios emergentes a amenazas que puedan afectar la relación entre el proveedor y HDI Seguros.

6.7.5. Gestión de eventos e incidentes de seguridad de la información

La gestión de eventos y de incidentes de seguridad de la información y ciberseguridad, tiene por objetivo establecer lineamientos para su identificación, clasificación, registro, análisis y tratamiento, así como para la documentación de las lecciones aprendidas y su notificación a las partes interesadas que intervienen en el procedimiento, considerando el tipo de la situación:

Tipo	Descripción
Eventos de seguridad de IT	Son los eventos que tienen relación al proceso de tecnología, los cuales se detectan por medio de alertas de seguridad arrojadas por las diferentes herramientas de monitoreo, por medio de recursos en la nube o cualquier otro software o aplicación que arroje alertas.
Evento de seguridad corporativa	Son los eventos que tienen relación con los procesos diferentes a IT pero que tienen injerencia en la seguridad de la información (ejemplo; incidentes informados a entes de control, PQRs - Peticiones, quejas y reclamos, proveedores, demás áreas etc.).
Evento de seguridad de la información	Cualquier situación que indica una posible infracción de seguridad de la información, que puede o no ser relevante y que no desencadena en un hecho que permita la materialización de un riesgo de seguridad de la información. (por ejemplo, el hurto o daño de un equipo de cómputo o dispositivo móvil, sospecha de phishing, etc.).
Incidente de seguridad de la información	Corresponde a un evento que si compromete seriamente la seguridad de la información con una probabilidad alta de afectar las operaciones de la compañía y materializar un riesgo (por ejemplo, información confidencial sin controles de acceso, expuesta de forma externa).
Incidente de seguridad de Inteligencia Artificial	Corresponde a una posible materialización de incidente de Inteligencia Artificial al interior y al exterior, por parte de un prestador de servicio a la compañía, donde se vea comprometida información o propiedad intelectual por un ataque descrito en el procedimiento de respuesta a incidentes.

- Reporte oportuno por medio de los canales establecidos por las Gerencias de Ciberseguridad, Cumplimiento y Talento y Cultura, informadas en; la presente Política, Código de ética, Reglamento Interno de Trabajo y cláusulas contractuales. Los canales de reporte serán, pero no se excluyen a: Mesa de ayuda, correo seguridadgobierno@hdiseguros y chats corporativos.
- El reporte se realizará acorde al procedimiento de manejo de incidentes definido por la compañía o el procedimiento de brecha de datos (data breach).

- Con lo anterior, solo los casos que tengan afectación directa a la seguridad de la información serán gestionados por la Gerencia de Ciberseguridad y el Comité de Seguridad de la Información de la compañía.
- Para los casos de los eventos que sean detectados por herramientas de monitoreo, se comunicara al cargo respectivo para gestionar la alerta y seguir el procedimiento de manejo de incidentes.
- El área de Ciberseguridad tomara los casos denunciados o presentados como ejemplos hipotéticos en las capacitaciones de concientización como parte de la educación continua a la organización.

6.7.6. Gestión de continuidad, respaldo y recuperación

Los lineamientos establecidos permiten preservar, restaurar y continuar con las operaciones de HDI Seguros sin afectaciones a las partes interesadas conservando la confidencialidad, integridad, disponibilidad y protección de la privacidad de la información.

Como parte fundamental de la continuidad del negocio o BCP, se deberán realizar pruebas periódicas de recuperación por el área de Riesgo Operativo, con el objetivo de obtener resultados exitosos, de no ser así, las áreas correspondientes tomarán medidas preventivas probadas hasta lograr un resultado satisfactorio, con el fin de que no ocurra un desastre o incidente para HDI Seguros y se logre reaccionar de inmediato ocasionando el mínimo riesgo posible y asegurando la estabilidad operacional.

Tanto para el DRP como para la continuidad de negocio se deberán establecer procedimientos por parte de las áreas respectivas que lo gestionan, que estarán disponibles en los casos de contingencia hasta que se resuelva la situación de riesgo y se normalice la operación, así como seguir los lineamientos establecidos en la "Política de Gestión de Incidentes de Seguridad y Ciberseguridad", la "Política de recuperación ante desastres" y "Política BCM - Plan de continuidad del negocio". Dichos procedimientos se deberán recrear por lo menos dos veces al año.

6.7.7. Gestión documental

Los lineamientos para la gestión documental que hagan parte del Sistema de Gestión de Seguridad de la Información (SGSI) se encontraran en el procedimiento respectivo apoyado por la Tabla de Control Documental y el repositorio del SGSI. Los documentos serán resguardados de acuerdo con la clasificación establecida, se revisará anualmente o bajo la necesidad de un cambio significativo, así mismo su archivo en el repositorio se contempla como una medida para la continuidad del sistema.

Los documentos deben pasar por un proceso de creación, elaboración, revisión, aprobación, archivo y publicación, estableciendo su conservación por un tiempo prudente y de acuerdo con la necesidad de compartir a un ente externo u autoridad. Los documentos también cuentan con un propietario designado el cual determinara el nivel de confidencialidad.

6.7.8. Gestión sobre la Inteligencia Artificial

Los lineamientos para la gestión de la inteligencia artificial en HDI Seguros, serán definidos dentro del documento “Política de uso de la inteligencia artificial” donde son descritos las obligaciones del negocio, Tecnología de la información y hacia proveedores de servicios, con inteligencia artificial, así como las guías que son proporcionadas por Talanx como requerimientos mínimos para el uso de esta tecnología.

Para las partes externas se ha contemplado los requerimientos contractuales requeridos para trabajar con la operación de HDI Seguros, al utilizar la tecnología de Inteligencia Artificial.

6.8. Gestión de personas

6.8.1. Gestión de preselección y selección de personal

Los objetivos establecidos en este punto hacen referencia a los controles aplicados antes y durante la contratación de personal a fin de establecer la idoneidad de la documentación entregada, antecedentes, conocimiento, experiencia con relación a un cargo al que aspira desempeñar, por mencionar algunos.

Se debe considerar que para este punto nos guiamos por el documento desarrollado por el área de Talento y Cultura, nombrado: “Política de selección, reclutamiento y salida de personal”.

6.8.2. Gestión de capacitación y concientización

Como parte de la preparación de algunas de nuestras partes interesadas (internos, outsourcing, intermediarios, clientes), se encuentra establecido el programa de capacitación del Sistema de Gestión de Seguridad de la Información (SGSI) y el calendario de concientización de Ciberseguridad, en el que se entrega información relevante para la toma de medidas básicas de seguridad, basados en los lineamientos de la "Política de capacitación y concientización".

6.8.3. Gestión de terminación o cambio de un empleo

Para el cambio o desvinculación de personal se establecen lineamientos que permitan desligar al personal saliente de cualquier acceso a los activos de la información de HDI Seguros y que a futuro la compañía se pueda ver afectada por la ocurrencia de un delito directa o indirecta del individuo.

Los cambios o modificaciones de cargos también deberán ser evaluados a fin de que el personal asuma las responsabilidades propias del nuevo rol y realice la entrega de cualquier información que ya no requiera para sus nuevas funciones.

Se debe considerar que para este punto nos guiamos por el documento desarrollado por el área de Talento y Cultura, nombrado: “Política de selección, reclutamiento y salida de personal”.

6.8.4. Gestión de trabajo remoto y/o hibrido

La gestión de trabajo remoto y/o hibrido aplica para el personal, terceros o proveedores de servicio que trabajen para o en representación de HDI Seguros, quienes se deben alinear a los requisitos de seguridad de la información establecidas para todo aquel que represente a la compañía en el marco de una relación contractual / laboral.

El personal que realiza trabajo remoto y/o hibrido tiene la responsabilidad de proteger los activos de la información asignados fuera de las instalaciones de HDI Seguros.

Para los casos en los que el trabajo se realice remoto y/o hibrido se debe realizar solo bajo el equipo de cómputo entregado por la compañía, no se permite trabajar bajo equipos propios.

En los contratos de trabajo o con relación de terceros se encontrarán las cláusulas y las responsabilidades del trabajo remoto y/o hibrido. Así mismo se debe considerar que para este punto nos guiamos por el documento desarrollado por el área de Talento y Cultura, nombrado: “Política de teletrabajo”.

Adicional en la "Política de Uso Aceptable de Activos de Información" se detallan otros lineamientos relacionados al Teletrabajo.

6.9. Gestión de controles físicos

6.9.1. Gestión de seguridad física y ambiental

El objetivo de la gestión de la seguridad física y ambiental corresponde a establecer medidas que permitan proteger los activos de la información que se encuentran de forma física. A continuación, algunos aspectos establecidos, en la "Política de Seguridad Física":

- Controles sobre el perímetro físico de la organización.
- Controles sobre el acceso físico a las oficinas.
- Ubicación de los activos físicos de la información, por ejemplo, los equipos de cómputo.
- Que desde el área de Infraestructura tecnológica se realicen monitoreos periódicos para el suministro constante de servicios de apoyo, como lo son: Servicios de internet, de energía, temperatura. etc.
- Mantenimiento y revisión de equipos de cómputo.
- Retiro físico de los activos de información que apliquen.
- Es responsabilidad de las personas, el cuidado frente a perdida, daño o deterioro de los activos de la información asignados. El detalle sobre el uso aceptable de los activos se encuentra definidos en su respectiva política.

- Esta política aplica a los centros de redes que se encuentran en las instalaciones de la compañía.
- Estos centros de cableado deberán mantener medidas mínimas de aseo y únicamente equipo y material del área de infraestructura y redes, no se puede almacenar en estos centros material distinto al antes mencionado.
- Se deberá mantener monitoreo adecuado a la temperatura, ingreso y egreso de los centros de datos y redes, para cumplir con las necesidades básicas de funcionamiento de los equipos tecnológicos que estén en las instalaciones de HDI seguros.
- Las instalaciones de la compañía en la que se encuentre cualquier activo de la información deberán contar con medidas para mitigar riesgos relacionados a desastres naturales (Inundaciones, terremoto, etc.), así como para situaciones accidentales o provocadas (incendios, vandalismo, etc.).

6.10. Gestión tecnológica

6.10.1. Gestión de uso de dispositivos

La gestión de uso de dispositivos esta alineada a su protección y definido en la "Política de Uso Aceptable de Activos de Información", así como los lineamientos de cómo se deberán comportar los usuarios con los activos de información que son proporcionados por parte de la compañía.

6.10.2. Gestión de vulnerabilidades

La gestión de vulnerabilidades tiene como principal objetivo la detección temprana de los posibles fallos o errores que pueden ser aprovechados por atacantes y por ende comprometer la confidencialidad, integridad, disponibilidad y protección de la privacidad de la información.

Se tiene mayor referencia para el manejo de vulnerabilidades en la “Política de Gestión de Vulnerabilidades”.

6.10.3. Gestión de uso de redes

La gestión de la seguridad de las redes se basa en controlar adecuadamente la información de los sistemas en los entornos críticos, restringiendo conexiones no autorizadas o publicas entre redes no confiables. Mayor referencia podrá ser encontrada en el documento “Política de Seguridad de Red”.

6.10.4. Gestión de contraseñas

Se establecen lineamientos para garantizar una adecuada gestión de contraseñas a través de su criptografía utilizando las mejores prácticas recomendadas a continuación:

- Se prohíbe bajo cualquier concepto compartir, ceder, y aceptar las contraseñas de otro usuario, ya que están son personales e intransferibles.

- Las credenciales de un servicio se deben dar de forma individual, indiferente del perfil que tenga asignado.
- Se recomienda el uso de gestores de contraseñas para el almacenamiento seguro de acceso a aplicaciones críticas.
- No utilizar la misma contraseña para varios sistemas, principalmente los críticos.
- Se debe utilizar donde esté disponible el doble factor de autenticación.
- Para mayor referencia se ha desarrollado la política “Política de Control de Acceso”.

6.10.5. Gestión de seguridad en los servicios en la nube

Para la gestión de seguridad en los servicios en la nube se establece los siguientes:

- Utilizar la encriptación como medio de protección de datos en reposo como en tránsito.
- Establecer gestión de identidades y accesos con el fin de controlar, conceder o denegar accesos para dar cumplimiento con el principio de menor privilegio.
- Implementar capas de protección como firewall u otros controles que sean necesarios para el análisis y el bloqueo de tráfico malicioso en la infraestructura de la nube.
- Llevar a cabo revisiones periódicas de la configuración de los recursos y servicios de la nube, garantizando el cumplimiento de los estándares y buenas prácticas de seguridad.
- Se deberá monitorear e implementar la realización de copias de seguridad en otra región de la misma nube u otra nube autorizada propiedad de la compañía. Esto será definido por el área de Infraestructura como dueño del DRP.

6.10.6. Gestión de desarrollo seguro

Para la puesta en producción de desarrollos se establecen lineamientos, con el fin de no afectar los datos consignados en los ambientes productivos de HDI Seguros.

- Se deben separar los ambientes de producción, desarrollo y pruebas con el fin de no alterar la información.
- Se deben seguir los lineamientos descritos en el documento “Política de Desarrollo Seguro”
- Se debe considerar este proceso para el desarrollo de tecnologías de Inteligencia Artificial, para el cual se contará con una política y procedimiento con buenas prácticas aceptables para HDI Seguros.
- Y otros definidos en la Política de Control de cambios de la compañía.

6.10.7. Gestión del cambio

Para la puesta en producción de cambios se establecen lineamientos, con el fin de no afectar los datos consignados en los ambientes productivos de las aplicaciones de HDI Seguros. Este proceso que ha sido

definido deberá seguir el documento "Política de Gestión de Cambios" de la compañía, que incluye no solo el desarrollo de aplicaciones, sino todo cambio en activos de la información que sean afectados.

Se debe definir un riesgo para los cambios, el cual debe considerar la criticidad de la data, criticidad del sistema, horario de ejecución, exposición del servicio a ambientes públicos.

6.11. Escenarios no previstos

Si durante la vigencia y revisión de este documento surgen escenarios que no esté contemplado en esta política, se deberá convocar al Comité de Seguridad de la Información para analizarlo, determinar su inclusión en la política y gestionar la excepción correspondiente. Tanto el Área de Riesgo Operativo como el propio Comité de Seguridad de la Información deberán estar informados sobre estas excepciones.

7. DOCUMENTOS ASOCIADOS

Nombre del documento	Tipo de documento	Ubicación del documento
Tabla de control documental SGSI	Matriz	Share Point
Declaración de Aplicabilidad (SOA)	Matriz	Share Point

8. GLOSARIO Y TÉRMINOS

8.1. Ciberseguridad: Término general para la actividad de gestión de riesgos que involucra la implementación, operación y mantenimiento de controles diseñados para cumplir con los requisitos comerciales de confidencialidad, integridad, disponibilidad y protección de la privacidad de los activos de información mediante la prevención de incidentes y/o la minimización de impactos.
8.2. Activo: Algo de valor para HDI Seguros. Puede ser tangible (por ejemplo, un edificio o un computador) o intangible (por ejemplo, el conocimiento, experiencia, saber hacer, información, software, datos).
8.3. Activos de información: Se refiere a cualquier elemento o recursos que tiene valor para la compañía y contiene o trata la información, como los sistemas informáticos, datos, base de datos, equipos de tecnología e información que requiere protección contra riesgos de ciberseguridad.
8.4. Confidencialidad: Uno de los tres elementos centrales de la ciberseguridad, junto con la disponibilidad y la integridad. La confidencialidad se refiere esencialmente al secreto o la privacidad.
8.5. Disponibilidad: Uno de los tres elementos centrales de la seguridad de la información y ciberseguridad, junto con la confidencialidad y la integridad. La disponibilidad se refiere al requisito de que los datos, sistemas, personas y procesos comerciales estén operativos y accesibles cuando la empresa los necesite.

8.6. Integridad: Uno de los tres elementos centrales de la ciberseguridad, junto con la confidencialidad y la disponibilidad. Propiedad de integridad y exactitud de los datos y sistemas informáticos. Protegido a través de controles como integridad referencial, validación de ingreso de datos, honestidad, ética y confianza.
8.7. Cumplimiento: Estado de conformidad con los objetivos de ciberseguridad y los controles definidos por HDI Seguros y/o por terceros (por ejemplo, las leyes, regulaciones de la industria y términos contractuales).
8.8. Dato sensible: Activo de información que se considera que tiene un riesgo especialmente alto de divulgación o modificación no autorizada (por ejemplo, un sistema que contiene datos personales o información de propiedad restringida). Los datos sensibles incluirán la siguiente información:

- Información de salud física o mental, incluida la información genética.
- Datos biométricos
- Información relacionada a la orientación sexual
- Información sobre antecedentes penales o condenas
- Multas administrativas o civiles, sanciones u otras sanciones
- Raza u origen étnico
- Inclinación política
- Inclinación religiosa
- Sindicatos

8.9. Dato privado: Dato que por su naturaleza intima o reservada es relevante para el titular.
8.10. Dato público: Dato que no contiene reserva alguna para su divulgación y por ende no genera afectación al titular.
8.11. Control: Algo que previene o reduce la probabilidad de un incidente de ciberseguridad, minimiza el daño causado, es decir, reduce o limita el impacto.
8.12. Riesgo: La probabilidad de que una amenaza de ciberseguridad explote una vulnerabilidad de ciberseguridad y cause un impacto. En otros contextos, los riesgos pueden ser comerciales, reglamentarios/legales, de mercado o de naturaleza personal, pero en este documento el "riesgo" se relaciona específicamente con la ciberseguridad.
8.13. Impacto: Un evento adverso causado por un incidente de seguridad cibernética, que genera pérdidas o costos directos o indirectos para HDI Seguros.
8.14. Probabilidad: Es la estimación de que ocurra o no sobre la materialización del riesgo.
8.15. Dispositivo: Un elemento de equipo informático o de red.
8.16. Control de Acceso: Tipo de control diseñado para restringir el acceso a un activo de información, permitiendo el acceso autorizado y evitando el acceso no autorizado.
8.17. BIA: Business Impact Analysis, en español Análisis de Impacto del Negocio. Es un proceso sistemático que evalúa los efectos potenciales de una interrupción de las operaciones comerciales críticas. Es una fase del plan de continuidad del negocio.
8.18. BCP: Business Continuity Plan, en español Plan de Continuidad del Negocio. Es un documento que describe los procedimientos que una empresa debe seguir para reanudar sus actividades críticas en caso de una interrupción. Es un plan integral para continuar operando, proteger la información y algunas veces hasta puede abarcar estrategias de reducción de costos a largo plazo.

8.19. DRP: Disaster Recovery Plan, en español plan de recuperación de desastres. Es un sistema que prepara a las organizaciones para posibles desastres que puedan dañar su infraestructura tecnológica es un documento que describe los procedimientos a seguir para reanudar el área de IT en caso de una interrupción.
8.20. Criptografía: La ciencia matemática detrás de la 'escritura secreta' que implica el uso de algoritmos matemáticos para transformar texto legible en texto cifrado ilegible y viceversa.
8.21. Encriptación: Aplicación de criptografía para hacer ininteligible la información para cualquiera que no tenga acceso a la clave correcta.
8.22. Desarrollo: Entorno informático que comprende sistemas, redes, dispositivos, datos y procesos de apoyo que utilizan los desarrolladores de software para desarrollar nuevos sistemas de aplicaciones (cf. entornos de producción o de prueba).
8.23. Control de Cambios: Proceso de gestión para proponer, revisar y aceptar o rechazar cambios en un proceso, sistema y/o la documentación asociada.
8.24. Dispositivo Móvil: Un dispositivo informático de bolsillo, que normalmente tiene una pantalla con entrada táctil o un teclado en miniatura. También conocido como dispositivo de teléfono celular, dispositivo de mano o computadora de mano.
8.25. Red: Significa un conjunto de enlaces o conexiones de comunicaciones de datos, más los nodos o dispositivos de red y los servicios en red que brindan. Los ejemplos incluyen enrutadores, cortafuegos, sistemas de aplicaciones, servidores de archivos, servidores web, servidores de correo y sistemas de administración de redes.
8.26. Vulnerabilidad: Control de ciberseguridad débil o faltante; debilidad inherente en un sistema o proceso.
8.27. Inteligencia Artificial (IA): Es una inteligencia basada en una serie de instrucciones entregadas a una maquina o programa informático para que realice análisis y/0 tareas estructuradas. Entre sus tipos se encuentra: (Aprendizaje Automático o ML, basados en Redes Neuronales e Inteligencia Artificial generativa).

6. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio
1.0	2025/03/28	Actualización del documento
2.0	2026/03/25	Se realizan modificaciones menores de redacción y se incluyen los lineamientos establecidos para la Inteligencia Artificial (IA).