POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN INTEGRADO

ÍNDICE

1. POLÍTICA

Esta política es una extensión de la política integrada, y orientada a la Seguridad de la Información.

AREA XXI, dentro de su equipo staff, cuenta con un equipo multidisciplinar, conformado por profesionales, con perfiles especializados y amplia experiencia, tanto en las distintas Áreas de Riesgo, como en los ramos en los que se desarrollan proyectos.

Los briefings de todo el equipo se encuentran en la página web de AREA XXI, en el link, https://www.area-xxi.com/quienes-somos/.

Sobre este mismo punto reseñar que, debido a la estructura de AREA XXI, su red de entidades colaboradoras y la línea de recruiting propia, puede organizar equipos adaptados a cada tipo de proyecto considerando sus especificaciones, bien por cantidad de recursos como por tipología de éstos.

El ser custodios de la información de sus clientes, preservar y hacer cumplir el principio de la Seguridad de la Información en sus operaciones es un compromiso asumido y permanentemente vigente para la compañía.

Por lo anterior, se ha decidido la instauración, mantención y mejoramiento continuo de un sistema, denominado Sistema de Gestión de Seguridad de la información (SGSI).

Este sistema permite instalar prácticas para garantizar que los riesgos de la seguridad de la información sean conocidos, adoptados, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en los riesgos y el contexto.

Lo anterior también aplica a los proveedores y colaboradores de AREA XXI ya que la prestación de su servicio contempla en algunos casos el manejo de información, en cualquiera de sus formas, o bien sus actividades se desarrollan en el entorno donde está almacenada esta información.

Se declara en la presente política la obligación de informar sobre incidentes de seguridad e intercambio de información relativos a dichos incidentes permitiendo la intervención de las autoridades competentes.

Es imprescindible contar con un marco general en el cual agrupar todos los subprocesos asociados a la Gestión de la Seguridad, comenzando por definir sus objetivos, el alcance o amplitud, los roles

y responsabilidades y el marco general para elaboración y revisión de las políticas de seguridad específicas para la información de AREA XXI.

La Alta Dirección se compromete a cumplir los requisitos aplicables en el marco legal, regulatorio y contractual, con el fin de mantener y mejorar el SGSI de acuerdo a esta Política de Seguridad de la Información de AREA XXI, integrando su establecimiento y supervisión mediante el funcionamiento del SGSI, asegurando que esta cubre los siguientes objetivos:

- Cumplir las expectativas de la Alta Dirección con respecto al correcto uso que el personal de AREA XXI, haga de los activos de información pertenecientes a la organización y sus clientes, como de las medidas y controles establecidos para el resguardo de los mismos.
- Establecer para todo el personal de AREA XXI la necesidad y obligación de salvaguardar la seguridad de la información, promoviendo la comprensión de sus responsabilidades individuales.
- Determinar las medidas esenciales de seguridad de la información que AREA XXI debe adoptar para protegerse apropiadamente contra amenazas que podrían afectar en alguna medida la confidencialidad, integridad y disponibilidad de la información, ocasionando alguna de las siguientes consecuencias: pérdida o mal uso de los activos de información (datos, equipos, documentación impresa, etc.), o interrupción total o parcial de los procesos que soportan el negocio.
- Cumplimiento con lo que la normativa vigente y en específico, las directrices que la Dirección General de Seguros y Fondos de Pensiones establezcan en relación con la Seguridad de la Información.

Además, con la implementación del Sistema de Seguridad de la Información, AREA XXI obtendrá una marca diferenciada frente a sus competidores que reforzará sus acciones comerciales aportando una ventaja competitiva, ampliará su mercado de actuación y le permitirá acceder a licitaciones en las que tener este Sistema de Gestión implementado sea un requisito de acceso.

Si bien esta política es la directriz principal y referencial, hemos desarrollado otras políticas más específicas, las cuales se detallan a continuación, y deben ser aplicadas según se indica en cada una

de ellas:

- SGSI-POL-001 Política de Seguridad de la Información (este documento).
- SGSI-POL-002 Política Dispositivos Móviles, Trabajo a Distancia y Dispositivos Extraíbles.
- SGSI-POL-003 Código de Conducta.
- SGSI-POL-004 Política de Control de Accesos y Gestión de Usuarios
- SGSI-POL-005 Política de Pantalla y Escritorio limpio.
- SGSI-POL-006 Política de Control de Proveedores y Socios.
- SGSI-POL-007 Política de Controles Criptográficos.
- SGSI-POL-009 Política de Desarrollo Seguro.
- SGSI-POL-010 Política Mantenimiento de Equipos y Servidores.
- SGSI-POL-011 Política de Prestación de Servicios en la Nube.
- SGSI-POL-012 Política Respaldo de Información.
- SGSI-POL-013 Política Uso y Resguardo de los Activos.
- SGSI-POL-014 Política de Ciberseguridad.
- SGSI-POL-015 Política de Protección y Privacidad de la Información Personal.
- SGCN-POL-001 Política de Continuidad del Negocio.

2. RESPONSABILIDADES

Las responsabilidades para el SGSI aplicadas son las siguientes:

- **Alta Dirección**
  - Revisar el SGSI al menos una vez por año o cada vez que se produzca una modificación significativa, informada por el CISO, y elaborar actas de dichas reuniones, con objeto de establecer la conveniencia, adecuación y eficacia del SGSI.
  - Aprobar las Políticas principales del Sistema de Gestión de Seguridad de la Información y Continuidad del Negocio:
    - SGSI-POL-001 Política de la Seguridad de la Información.
    - SGCN-POL-001 Política de Continuidad del Negocio.
    - SGSI-POL-003 Código de Conducta.
- **El Oficial de Seguridad de la Información (CISO) (*Chief Information Secutiry Officer*)**
  - Coordinar la operativa del SGSI, e informar y reportar sobre su desempeño.
  - Otorgar a los activos la protección de la integridad, disponibilidad y confidencialidad según el inventario de activos, responsabilidad del PMO, o de quien se haya determinado.
  - Debe ser informado de todos los eventos, incidentes o vulnerabilidades de seguridad que pudiesen ocurrir.
  - Definir qué información relacionada con la seguridad de la información será comunicada a qué parte interesada, tanto interna como externa, por quién y cuándo.
  - Adoptar e implementar el Plan de capacitación y concienciación de la Seguridad de la Información, que corresponde a todas las personas, tanto internas como externas, que cumplen una función en la gestión de la seguridad de la información.
  - Revisar la documentación inherente al Sistema de Gestión de Seguridad de la Información y Continuidad del Negocio, elaborada por los colaboradores del SGSI/CN.

- **Comité de Seguridad de la Información y Continuidad del Negocio (CSI)**
  - Asegurar que el SGSI sea implementado y mantenido de acuerdo con esta Política y de asegurar que todos los recursos necesarios estén disponibles.
  - Revisar los incidentes de seguridad y la operación del sistema según acta de constitución.
  - Velar por la implementación de programas de capacitación y concienciación de empleados sobre seguridad de la información.
  - Aprobar la documentación relacionada con el Sistema de Gestión de Seguridad de la Información y Continuidad del Negocio, excepto en los casos en que dicha responsabilidad le corresponda a la Alta Dirección.
- **Colaboradores del SGSI/CN (CSGSICN)**
  - Elaborar la documentación inherente al Sistema de Gestión de Seguridad de la Información y Continuidad del Negocio, en colaboración con el CISO.
  - Realizar cualquier otra labor que les sea encomendada, en el marco de su responsabilidad, relativa al Sistema de Gestión de Seguridad de la Información y Continuidad del Negocio.

3. COMUNICACIÓN E INFORMACIÓN

La presente Política será comunicada a todo el equipo de AREA XXI, y terceras partes relevantes, en su caso, siendo así mismo publicada en la intranet, o en el repositorio digital de la compañía para facilitar su acceso, dentro del marco general y de los programas de formación y concienciación, en relación al SGSI (Sistema de Gestión de Seguridad de la Información).

En el fichero SGSI-REG-018 Registro Matriz de Partes Interesadas se recoge la información detalla de las partes interesadas y la forma apropiada de involucración de cada una de ellas en el SGSI de AREA XXI.

Así mismo, cualquier hecho relevante que afecte al cumplimiento de alguna de las obligaciones contempladas en la misma, deberá ser informado de forma expresa a los implicados, así como a los responsables de las distintas Áreas y a la Alta Dirección, quedando constancia por escrito de dichas comunicaciones.

4. REVISIÓN DE LA POLÍTICA

La presente Política será revisada por el Responsable de Seguridad de la Información (CISO), como encargado de la coordinación operativa del SGSI, con el fin de asegurar que se mantiene su idoneidad, adecuación y eficacia, o en caso de que se produzca algún cambio significativo en lo que concierne a este sistema, y como mínimo una vez al año.

Si en algún momento se produce una modificación, será incorporada a este documento, y aprobada por el CSI, quedando reflejados los cambios en el cuadro del histórico de versiones siguiente.

5. HISTÓRICO DE VERSIONES

Versión	Fecha	Descripción del Cambio	Responsable del cambio	Responsable de aprobación	Fecha de aprobación
00	Julio 2021	Creación del documento	Implementación	No aplica	Julio 2021
01	Septiembre 2021	Actualización del documento Inclusión Punto 2 - Responsabilidades	CISO	Alta Dirección	Septiembre 2021
02	Marzo 2022	Actualización tras Fase I de certificación	CISO	Alta Dirección	Marzo 2021