


| CONTROL DE VERSIONES | | | |
|----------------------|--|--|----------------------|
| Versión | Autor(es) Ordenados alfabéticamente | Descripción de la versión | Fecha de elaboración |
| Versión 1.0 | Dirección | Documento inicial | 01/04/2021 |
| Versión 2.0 | Dirección | Relación con otras políticas de seguridad de la información | 27/06/2022 |
| Versión 3.0 | Dirección | Alcance de la ciberseguridad | 10/10/2022 |
| Versión 4.0 | Dirección | Inclusión de principios de ciberseguridad y directrices nube | 24/01/2023 |

TABLA DE CONTENIDO

| | | |
|---------------|--|----------|
| 1 | <i>Definiciones</i> | 2 |
| 2 | <i>Política De Ciberseguridad</i> | 3 |
| 2.1. | <i>Alcance</i> | 3 |
| 2.2. | <i>Principios De Ciberseguridad</i> | 4 |
| 2.2.1. | <i>Prevención</i> | 4 |
| 2.2.2. | <i>Compromiso de la Dirección:</i> | 4 |
| 2.2.3. | <i>Responsabilidad compartida</i> | 5 |
| 2.2.4. | <i>Formación:</i> | 5 |
| 2.2.5. | <i>Cumplimiento normativo:</i> | 5 |
| 2.2. | <i>Organización de Ciberseguridad</i> | 6 |

| | | |
|--|--|---------------|
|  Paradigma | Política del Sistema de Gestión Integral | SGSI-PO-02 |
| | Política de Ciberseguridad | Versión: 4.0 |
| | Este documento es para uso Interno | Página 2 de 8 |

1 Definiciones


Ciberseguridad:

Ciberseguridad es la práctica de proteger los sistemas críticos o importantes y la información confidencial de los ataques digitales. Integra un conjunto de políticas, conceptos de seguridad, recursos, controles de seguridad, métodos de gestión del riesgo, acciones, investigación, desarrollo, formación y buenas prácticas en general, utilizadas para proteger los datos, así como también, para combatir las amenazas contra las redes, aplicaciones e infraestructura, ya sea que esas amenazas se originen dentro o fuera de una organización. Una estrategia de ciberseguridad apoyada en una buena organización y regida por las mejores prácticas y lo más automatizada posible, se dirige más a combatir las ciberamenazas que a llevar a cabo procesos de recuperación ante la ocurrencia de ataques materializados, por lo tanto, es más efectiva y reduce el ciclo de vida y costos.

Ciberespacio:

El ciberespacio es un ambiente no físico en donde interactúan los seres humanos, el software y los servicios que en Internet se ofrecen. (ISO 27032).

El ciberespacio es un ambiente complejo resultante de la interacción de las personas, el software y los servicios de Internet soportados estos por el hardware y las redes de comunicaciones (ISO 27032).

| | | |
|--|--|---------------|
|  Paradigma | Política del Sistema de Gestión Integral | SGSI-PO-02 |
| | Política de Ciberseguridad | Versión: 4.0 |
| | Este documento es para uso Interno | Página 3 de 8 |

La seguridad en Internet y en el ciberespacio nos convoca a todos. La presencia actual de las organizaciones en este espacio crea unos beneficios, pero también unos riesgos. (Contexto de ISO 27032).

La convergencia de las tecnologías de información y de las comunicaciones han propiciado diferentes tipos de ataques cada vez más sofisticados.


2 Política De Ciberseguridad

2.1. Alcance

Esta política tiene como propósito hacer que los lineamientos operativos, tecnológicos, de organización y de seguridad, funcionen en conjunto, para garantizar que las posibilidades de un ataque cibernético sean limitadas y, si se materializa, el equipo de TI, de seguridad, los dueños de proceso y la Dirección, cuenten con el conocimiento necesario para limitar el daño.

Para PARADIGMA es prioritario proteger los activos de información de la empresa, de nuestros clientes y demás partes interesadas, a nivel físico y digital, integrando y/o configurando plataformas tecnológicas y aplicaciones seguras, que garanticen la seguridad de punta a punta.

La política cubre los activos de información de la empresa, de los clientes y de las partes interesadas y está dirigida a todo el personal de PARADIGMA, a proveedores y terceros que tengan algún vínculo con los

| | | |
|--|--|---------------|
|  Paradigma | Política del Sistema de Gestión Integral | SGSI-PO-02 |
| | Política de Ciberseguridad | Versión: 4.0 |
| | Este documento es para uso Interno | Página 4 de 8 |

procesos de la empresa o que, por motivos del negocio, tengan acceso a información sensible de PARADIGMA o de nuestros clientes. La política deberá ser aplicada en el ejercicio de las funciones de cada colaborador o proveedor, teniendo en cuenta sus responsabilidades frente a la seguridad de la información y ciberseguridad, establecidas en la política *SGSI-PO-01 Capítulo 6 – Organización de Seguridad de la Información.*

2.2. Principios De Ciberseguridad


En PARADIGMA La gestión de ciberseguridad, está regida por los siguientes principios:

2.2.1. Prevención:

Se deben potenciar las capacidades, para lograr proteger los activos de información y detectar anticipadamente las ciberamenazas, para evitar su materialización, o en el caso en que suceda, se pueda minimizar sus efectos.

2.2.2. Compromiso de la Dirección:

En PARADIGMA se asume el Gobierno y la gestión de ciberseguridad, como funciones cuya responsabilidad se ejerce en todos los niveles de la organización, comenzando por la Dirección, de tal manera, que todos los comités en los se contemple el propósito de salvaguardar los activos de información bajos los principios de seguridad y ciberseguridad, principal o secundario, sea salvaguardar los activos de información balos los en cabeza de un representante de la Dirección, forma que el Comité de Dirección asume el compromiso de

| | | |
|--|--|---------------|
|  Paradigma | Política del Sistema de Gestión Integral | SGSI-PO-02 |
| | Política de Ciberseguridad | Versión: 4.0 |
| | Este documento es para uso Interno | Página 5 de 8 |

asegurar la implantación del sistema de gestión de la ciberseguridad que permita llevar a la práctica lo definido en el presente documento.

2.2.3. Responsabilidad compartida:


La ciberseguridad es una responsabilidad en la que se requiere la colaboración y compromiso pleno de toda la organización, incluyendo los clientes y demás partes interesadas, tanto en lo que se refiere al cumplimiento de las políticas de seguridad de la información, los acuerdos contractuales y procedimientos establecidos, como a la colaboración incondicional y oportuna que se requiera ocasionalmente por parte de la Dirección, oficial de seguridad, integrantes de TI, dueños de procesos, integrantes de los diferentes comités y líderes de las empresas cliente.

2.2.4. Formación:

La Dirección de PARADIGMA es consciente de que uno de los pilares indispensables para la correcta gestión de la ciberseguridad, es un adecuado nivel de formación, sensibilización y concienciación, por lo cual, promueve una cultura de ciberseguridad mediante acciones de formación dirigidas a todos los colaboradores y grupos de interés implicados. Así mismo, garantiza que los equipos de ciberseguridad disponen de los conocimientos, experiencia y capacidades tecnológicas para cumplir con los objetivos de ciberseguridad de la empresa.

2.2.5. Cumplimiento normativo:

Es compromiso de la Dirección garantizar que toda la organización cumpla las normas, reglamentaciones y regulaciones, que en materia de ciberseguridad, establezcan los entes de control.

| | | |
|--|--|---------------|
|  Paradigma | Política del Sistema de Gestión Integral | SGSI-PO-02 |
| | Política de Ciberseguridad | Versión: 4.0 |
| | Este documento es para uso Interno | Página 6 de 8 |


2.2. Organización de Ciberseguridad

En el *Manual de Seguridad de la Información y Ciberseguridad SGSI-MS-01*, se relaciona la estructura orgánica de seguridad de la información y Ciberseguridad de PARADIGMA. La estructura está encabezada por el Gerente Ejecutivo, como representante de la Dirección, quien delega la dirección de ciberseguridad en el Oficial de Seguridad y el Jefe de TI, con el apoyo de las demás jefaturas y de todo el personal, puesto que en la definición de cada perfil de la empresa, se establecen las responsabilidades asociadas a seguridad de la información y ciberseguridad.

Para PARADIGMA es fundamental la protección de la información, tanto en el ámbito físico como en el virtual, con el propósito de salvaguardar los intereses de la empresa y de las partes interesadas, de ahí que el Sistema de Gestión Integral está alineado con las Normas *ISO 27001 Seguridad de la Información* e *ISO 27032 Guía de Ciberseguridad*, como marco seguro para el intercambio de información, el manejo de incidentes y la coordinación para hacer más seguros los procesos.

En PARADIGMA trabajamos en pro de prevenir impactos que afecten o generen pérdidas a la organización y partes interesadas; por lo cual identificamos, controlamos y monitoreamos todo evento que tenga una probabilidad potencial de materializarse y poner en riesgo la información como activo fundamental, en el marco de los principios de confidencialidad, integridad y disponibilidad y cubriendo los siguientes aspectos:


- Seguridad de las redes

| | | |
|--|--|---------------|
|  Paradigma | Política del Sistema de Gestión Integral | SGSI-PO-02 |
| | Política de Ciberseguridad | Versión: 4.0 |
| | Este documento es para uso Interno | Página 7 de 8 |

- Seguridad de las aplicaciones
- Seguridad de la información
- Seguridad operativa
- La recuperación ante desastres y la continuidad del negocio
- La capacitación del usuario final

En este sentido, la Dirección establece las siguientes directrices de ciberseguridad, complementando de esta forma la Política Integral de los Sistema de Gestión de la Empresa y las demás políticas, con el propósito de salvaguardar los activos de información en entornos físicos y de red, en nubes públicas o privadas, incluidas las conexiones establecidas en Internet, atendiendo los siguientes aspectos de estricto cumplimiento:

- Garantizar los principios de Confidencialidad, Integridad y Disponibilidad de los activos de información mediante la aplicación de las políticas de la empresa, llevando una adecuada gestión de riesgos, eventos e incidentes de seguridad y asegurando el desempeño de las plataformas tecnológicas.
- Gestionar la mitigación de riesgos siguiendo las estrategias establecidas en ISO 27032: Detección, Preparación y Respuesta y estableciendo controles a nivel de servidores, aplicaciones, usuario final e ingeniería social.
- En proyectos cuya arquitectura sea configurada en nubes públicas, se deberá seleccionar un proveedor que cuente con medidas y herramientas para la prevención, detección y acción ante los ciberataques, así como también, que garanticen la toma de backups diarios de forma automática cada día, garantizando el restablecimiento de la operatividad de la empresa en menor tiempo.

| | | |
|--|--|---------------|
|  Paradigma | Política del Sistema de Gestión Integral | SGSI-PO-02 |
| | Política de Ciberseguridad | Versión: 4.0 |
| | Este documento es para uso Interno | Página 8 de 8 |

- Las nubes públicas seleccionadas, deberán dar garantía de cumplimiento de la Norma *ISO 27017 Directrices sobre los controles de seguridad de la información correspondientes al aprovisionamiento y uso de servicios en la nube* e *ISO 27018 Prácticas para proteger datos personales en la nube*, *ISO 27701 Gestión de la privacidad de la información*, así como también, deberán estar en condiciones de facilitar los informes de control interno sobre los servicios que prestan, esto es, los informes SOC1, SOC2 y SOC3.
- Definir e implementar controles informáticos robustos para mitigar ataques cibernéticos conocidos, a los que se encuentran expuestas las aplicaciones y plataformas tecnológicas de la organización.
- Planear, ejecutar y mantener planes de auditoría, con el propósito de verificar la adecuada implementación de los controles de seguridad y ciberseguridad en las plataformas tecnológicas.
- Programar periódicamente con una empresa especializada, la ejecución de test de vulnerabilidad técnica a la plataforma tecnológica de la empresa, tratando los riesgos asociados y remediando prontamente las vulnerabilidades identificadas, comenzando con las de mayor criticidad.
- Establecer contactos de la industria de la ciberseguridad para hacer frente a ataques de día cero.