ORION

5.2 P01 Seguridad de la información

Sistema de Gestión de Seguridad de la Información y Calidad

Julio 2024

USO INTERNO

Fecha Vigencia: ***18/07/2024***

Versión: ***13***

Índice

1. Información del Documento.

HISTORIA DEL DOCUMENTO	
Nombre del Documento:	5.2 P01 Seguridad de la Información
Creado por:	Oficial de Seguridad
Responsable del Documento:	Oficial de Seguridad
Fecha de la Creación	14 de Junio de 2013
Aprobado por:	Comité de Calidad y Seguridad
Fecha de la Aprobación:	28 de Junio de 2013

CONTROL DE VERSIONES

Versión	Fecha de Vigencia	Aprobación	Detalle
001	28 de Junio de 2013	Comité de Calidad y Seguridad	Creación del documento. Primera versión.
002	14 de Marzo de 2014	Comité de Calidad y Seguridad	Cambio de sección en el SGSI-C, según versión 2013.
003	21 de Enero de 2015	Comité de Calidad y Seguridad	Actualización del formato de los documentos del SGSI-C.
004	28 de octubre de 2016	Comité de Calidad y Seguridad	Revisión del documento.
005	17 de noviembre de 2017	Comité de Calidad y Seguridad	Revisión del documento.
006	07 de junio de 2018	Comité de Calidad y Seguridad	Revisión del documento.
007	04 de Marzo de 2019	Comité de Calidad y Seguridad	Actualización del formato de los documentos del SGSI-C.
008	16 de Septiembre 2020	Comité de Calidad y Seguridad	Actualización de las políticas
009	26 de Marzo 2021	Comité de Calidad y Seguridad	Actualización de las políticas
010	24 de Junio de 2022	Comité de Calidad y Seguridad	Revisión del documento.
011	27 de febrero 2023	Comité de Calidad y Seguridad	Alineamiento de política y objetivos

012	31 de mayo de 2023	Comité de Calidad y Seguridad	Revisión del documento.
013	18 de julio de 2024	Comité de Calidad y Seguridad	Revisión del documento.

2. Introducción

Orión es una empresa que presta servicios especializados, orientados a proporcionar soluciones de seguridad de la información a sus clientes. Como tal, la gerencia reconoce la importancia y el valor cada vez mayor de la información con respecto al funcionamiento eficiente y efectivo de la organización. La información no es sólo crítica para el éxito del negocio, sino estratégica para su supervivencia a largo plazo. Por esta razón, se establece la siguiente política de la Empresa, orientada a definir las medidas que resguarden la confidencialidad, integridad y disponibilidad de la información propia de la empresa así como la de sus clientes.

.

3. Objetivos

La política de seguridad de la información posee los siguientes objetivos:

- Crear un marco referencial para gestionar de manera apropiada la seguridad de la información y ciberseguridad de la Empresa y de sus clientes, y proporcionar a todo el personal de la Empresa los lineamientos que faciliten la toma de decisiones apropiadas relacionadas con la seguridad de la información y ciberseguridad.(ver 7.1, 7.3 y 7.8).

- Establecer las expectativas de la gerencia con respecto al uso que el personal debe hacer de los activos de información de la Empresa, así como de las medidas que se deben adoptar para la protección de estos recursos. (ver 7.2).

- Infundir en todo el personal de la empresa la conciencia de la necesidad de la seguridad de la información, ciberseguridad y la comprensión de sus responsabilidades individuales. (ver 7.7).
- Especificar las medidas esenciales de seguridad de la información y ciberseguridad que la Empresa debe adoptar, para protegerse apropiadamente contra amenazas que podrían afectar la confidencialidad, integridad y disponibilidad de la información, ocasionando alguna de las siguientes consecuencias: (ver 7.4, 7.5 y 7.6).
    - Pérdida o mal uso de los activos.
    - Pérdida de imagen como empresa especializada en seguridad.
    - Pérdidas para el negocio.

4. Alcances y Limitaciones

Esta política debe ser cumplida por todo el personal de la Empresa y los terceros autorizados para acceder a los activos de la organización.
La gestión de la seguridad de la información debe abarcar a todos los activos de información que la empresa posea en la actualidad o en el futuro, de manera que la no inclusión explícita en el presente documento no constituye argumento para no proteger activos de información que se encuentren en otras formas. La política cubre toda la información impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o usando medios electrónicos, mostrada en películas o hablada en una conversación.

La gestión de la seguridad de la información debe estar alineada con los requerimientos definidos en el estándar ISO/IEC 27001:2013 y las buenas prácticas definidas en el estándar ISO/IEC 27002:2013, además de los requisitos legales, normativos y contractuales relativos a seguridad de la información que sean aplicables a la organización.

Considerando que los recursos son limitados y deben ser utilizados aplicando criterios de buen uso, la gestión de la seguridad de la información se formalizará para proteger en primer lugar los procesos más críticos del negocio, extendiéndose eventualmente a toda la organización.

5. Definiciones

A continuación se definen algunos conceptos que deben estar claros para dar un cumplimiento apropiado a la presente política.

- **Activo:** Es cualquier elemento que tenga valor para la organización.
- **Información:** Es la interpretación que se da a los datos. En el caso de la presente política, se entiende como información a toda forma que contenga datos relacionados con los negocios de la Empresa, así como antecedentes proporcionados por los clientes en el contexto de la prestación de servicios.
- **Confidencialidad:** Es la propiedad de que la información no es puesta a disposición o divulgada a individuos, entidades o procesos no autorizados.
- **Integridad:** Es la propiedad de asegurar la completitud y exactitud de los activos.
- **Disponibilidad:** Es la propiedad de estar accesible y usable cuando una entidad

autorizada lo solicite.

- **Seguridad de la Información:** Es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Ciberseguridad:** Es la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.
- **Buen uso:** Es el uso de los activos que se realiza teniendo presentes las expectativas de la Empresa, esto es:
    - Evitando el mal uso o abuso de los activos.
    - Cumpliendo las políticas, estándares y procedimientos que la organización defina.
- **Evento de seguridad: Es cualquier situación que indica:**
    - Una posible violación a la política de seguridad de la información.
    - La falta de medidas de protección.
    - Una situación previamente desconocida que puede ser relevante para la seguridad.

- **Incidente de seguridad:** Uno o más eventos de seguridad que tienen una alta probabilidad de:
    - Comprometer las operaciones de negocio.
    - Amenazar la seguridad de la información.
- **Sistema de gestión de la seguridad de la información:** Es la parte del sistema de gestión general, que considera los riesgos del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
- **Usuario:** Es toda persona a la cual se le concede autorización para acceder a la información y a los sistemas de la Empresa. Incluye al personal de la Empresa, que puede ser interno o externo a la empresa, y los terceros.
- **Tercero:** Se refiere a personas externas a la empresa que pertenecen a alguna de las siguientes categorías:
    - **Proveedor:** Se refiere a empresas prestadoras de servicios, las empresas contratistas, subcontratistas y cualquiera que, por cuenta propia o de terceros, desarrolle trabajos para o por cuenta de la Empresa.
    - **Cliente:** Es toda empresa que contrate servicios de cualquier naturaleza a la Empresa.
    - **Visitante:** Es cualquier persona externa a la empresa, que no es ni proveedor ni cliente, a la cual se le autoriza de manera restringida el acceso a los recursos o instalaciones de la Empresa. Caen en esta categoría: familiares o amigos de empleados, socios de negocios, clientes potenciales, auditores y vendedores.

6. Responsabilidades Generales

- **Gerente General:** Es el responsable final de la existencia y cumplimiento de las medidas para mantener un nivel de seguridad de la información acorde con el rol de la empresa y los recursos disponibles.
- **Oficial de Seguridad:** Es el representante del Gerente General en la definición y aplicación de los criterios de seguridad de la información en la Empresa, para lo cual:
    - Debe validar que los activos son identificados y valorizados apropiadamente por sus Propietarios, y que este valor se mantiene actualizado en el tiempo.
    - Debe analizar permanentemente el nivel de riesgo existente, proponiendo a la gerencia soluciones costo-efectivas.
    - Una vez autorizada la implementación de las medidas de protección, debe coordinar con los supervisores su materialización oportuna y correcta.
    - Además es el responsable de mantener actualizadas las políticas de seguridad y de difundirlas al personal de la Empresa y a terceros.
- **Comité de Seguridad:** Es el grupo formado por los gerentes de primera línea, que tiene por responsabilidad asesorar al Gerente General en cuanto a la gestión de la seguridad de la información, en coordinación con el Oficial de Seguridad.
- **Personal de la Empresa:** Tiene la responsabilidad de cumplir con lo establecido en este documento y aplicarlo en su entorno laboral. Además, tiene la obligación de alertar de manera oportuna y adecuada a su supervisor, cualquier situación que atente contra lo establecido en esta política o pueda poner en riesgo la seguridad de la información.
- **Supervisor:** Es toda persona encargada de un grupo de personas, área o gerencia en la Empresa. Es responsable de que las personas a su cargo cumplan con las políticas y principios de seguridad definidos. Permanentemente debe preocuparse de identificar incidentes, debilidades y riesgos que afecten a los activos de su área, y canalizarlos al Oficial de Seguridad para que sean gestionados y se tomen las medidas correspondientes.
- **Propietario de la Información:** Es el responsable de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos. Debe participar activamente en la definición del valor de la información para el negocio, de manera que se puedan definir los controles apropiados para protegerla.
- **Custodio de la Información:** Es cualquier persona que mantiene bajo su responsabilidad información de la cual no es el Propietario. Es responsable de aplicar las medidas de seguridad que se definan de acuerdo al valor de los activos. En esta categoría se encuentra:
    - El personal encargado de los sistemas de tecnologías de información que crean, procesan o modifican la información de la Empresa y sus clientes.
    - El personal que maneja información de los clientes de la Empresa.

- El personal administrativo que maneja información de la Empresa y sus clientes.

7. Seguridad de la Información

7.1 Adhesión a la política

- La presente política y los estándares y procedimientos que tenga asociados, deben ser cumplidos por todo el personal, sin excepción.
- El Oficial de Seguridad debe monitorear el cumplimiento de la presente política, reportando los resultados a la gerencia, en el Comité de Calidad y Seguridad.
- La gerencia de la Empresa se reserva el derecho de revocar a los usuarios el privilegio de acceso a la información y a las tecnologías que la soportan.
- La gerencia de la Empresa se reserva el derecho de tomar medidas disciplinarias al personal que falte a lo aquí dispuesto.

7.2 Protección de la Información

- La gerencia de la Empresa reconoce que la seguridad de la información y la ciberseguridad es un objetivo del negocio, que debe ser impulsado y apoyado por todos los miembros de la organización.
- **La información es un activo valioso que debe ser protegido** de manera consistente con los objetivos del negocio, y los requerimientos legales, normativos y contractuales que sean aplicables.
- Se debe tener presente que no es posible eliminar el riesgo, sólo controlarlo, por lo tanto las medidas que se definan para proteger la información **deben ser determinadas en base a un análisis previo** que considere el **costo beneficio** de aplicarlas en relación con los riesgos existentes.
- Periódicamente, al menos una vez al año, deben realizarse **análisis de riesgos** sobre los activos, de manera que se definan **controles** de seguridad apropiados al valor de los activos de información.

7.3 Apoyo Gerencial

- La gerencia de la Empresa **debe destinar los recursos necesarios** para asegurar que todo el personal reciba **entrenamiento permanente** en seguridad de la información, de acuerdo a su función y rol en la empresa.

- Los riesgos que se identifiquen deberán ser **gestionados por la gerencia** de manera que sean llevados a un **nivel aceptable** para el negocio. Para esto podrán ser aceptados, eludidos, transferidos o mitigados.
- Para aquellos riesgos que no sean aceptables, deberán seleccionarse medidas de protección apropiadas, las cuales serán sometidas a la **aprobación de la gerencia** para asegurar que:
    - Son suficientes para llevar el riesgo a un **nivel apropiado.**
    - Tienen un **costo** apropiado al **beneficio** que aportan.
    - Reciben los **recursos y el apoyo necesarios** para su implementación.

7.4 Clasificación de la Información

- Los Propietarios de la información deben clasificar la información que esté bajo su responsabilidad en **"Confidencial"**, de **"Uso Interno"** o **"Pública"**, de acuerdo a su importancia para el negocio.
- Toda la información que no haya sido clasificada debe considerarse como de **"Uso Interno"** de manera que reciba los niveles de protección acordes a esta clasificación.
- El Oficial de Seguridad debe preocuparse de que la información **reciba una clasificación apropiada**, de manera que las medidas de protección que se apliquen corresponden a las necesidades reales del negocio.
- Por cada uno de los niveles de clasificación establecidos, se deben definir **medidas de protección específicas**, las que serán aplicadas por todo el personal.

7.5 Uso de la Información

- Todo uso de activos de información debe ser para propósitos del negocio de acuerdo a las políticas, estándares y procedimientos que se definan y considerando criterios de buen uso.
- La Empresa permite el uso personal de algunos activos, siempre que éste sea moderado y no sea una actividad maliciosa o negligente que afecte el funcionamiento normal del negocio.
  Asimismo, los usuarios de activos son responsables de:

- No divulgar información de la Empresa ni de sus clientes, que haya sido clasificada como "Confidencial" o de "Uso Interno", salvo que hayan sido expresamente autorizados por el Propietario de la Información quien deberá hacerse responsable de esta divulgación.
- Solicitar autorización por escrito al Propietario de la Información, cuando necesiten proporcionar información "Confidencial" o de "Uso Interno" a terceros. La entrega de esta

información se realizará suscribiendo acuerdos de confidencialidad con el tercero y aplicando los controles específicos que se definan.

- Cumplir con todos los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo las políticas de seguridad que deberán mantenerse alineadas con las leyes vigentes.
- Proteger sus elementos de control de acceso, como contraseñas y tarjetas de identificación, ya que son individuales, intransferibles y de responsabilidad única de cada empleado.

  Reportar a un nivel apropiado y lo antes posible, cualquier incidente que ponga en riesgo la seguridad de la información y/o ciberseguridad para que se tomen las medidas necesarias.

7.6 Criterio de Clasificación de Información

A continuación se indica el criterio que debe ser aplicado para clasificar la información y las medidas mínimas para su tratamiento.

Clasificación	Descripción	Tratamiento
Confidencial	Es toda aquella información que tiene el potencial de afectar en forma grave el prestigio de la empresa y su continuidad en el negocio. En esta categoría está: ● Información de clientes. ● Información relacionada con planes estratégicos, metodologías propietarias y procedimientos de trabajo. ● Cualquier otra información cuyo propietario estime necesario un nivel de protección superior.	Debe ser protegida de manera que sólo las personas autorizadas puedan accederla. Sólo debe ser accedida por algunas personas, las cuales deben estar definidas previamente en un inventario de activos de información. En el caso de los documentos, debe indicarse en ellos qué personas están autorizadas a verlos. Si otra persona requiere acceso, este deberá ser autorizado explícitamente por el Propietario de la Información respectiva.
Uso Interno	Es toda aquella información cuya divulgación, adulteración y/o destrucción, sin generar un daño grave a la empresa, puede producir pérdida de tiempo para su recuperación, afecte la imagen en forma menos grave o disminuya las posibilidades de éxito en propuestas comerciales. En esta categoría está: ● Información de clientes que hayan solicitado en forma explícita su tratamiento como tal.	Sólo debe ser accedida por personal de la Empresa. Si otra persona requiere acceso, éste deberá ser autorizado explícitamente por el Propietario de la Información respectiva. NOTA: Se debe tener presente que toda la información de la Empresa cae en esta categoría a menos que haya sido explícitamente clasificada como “Confidencial” o “Pública”.

	• Información cuyo propietario requiera un nivel moderado de protección. • Información sobre problemas o incidentes de seguridad.	
Pública:	Información que, por su naturaleza, no presente riesgos para la empresa y que pueda ser dada a conocer al público en general. En esta categoría está: • Publicidad de la Empresa. • Información del Sitio Web y material de marketing.	Puede ser entregada libremente a terceros.

7.7 Compromiso con la Seguridad de la Información

Orión se compromete a satisfacer los requisitos aplicables, relacionados a la seguridad de la información y ciberseguridad.

7.8 Compromiso con la mejora continua

Orión se compromete a mejorar continuamente su sistema de Gestión de seguridad de la información.
Para ello utilizará como input: Las auditorías internas y externas, los resultados de la revisión por la alta dirección, la revisión de los incidentes de seguridad y las situaciones internas y externas que puedan afectar al SGSI-C.

8. Documentación de Referencia

La gerencia publicará documentos adicionales para detallar las medidas de seguridad que se definan. Estos documentos tendrán como mínimo la clasificación de “Uso Interno” y deberán ser conocidos exclusivamente por el personal que esté involucrado en su cumplimiento.

Dichos documentos, estarán distribuidos en las áreas de la seguridad de la información que se indican a continuación:

- Política de seguridad.
- Organización de la seguridad de la información.
- Equipos Móviles y teletrabajo
- Seguridad de los recursos humanos.
- Gestión de activos

- Control de acceso.
- Criptografía.
- Seguridad física y ambiental.
- Seguridad de las operaciones.
- Seguridad de las Comunicaciones.
- Adquisición, desarrollo y mantención de sistemas de información.
- Relación con los proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de Seguridad en la Gestión de la continuidad del negocio.
- Cumplimiento.

9. Aprobación General

La presente política entra en vigencia a partir del 24 de marzo de 2022, según lo acordado en el Comité de Calidad y Seguridad.

10. Disposiciones Finales

10.1 Implementación y Cumplimiento

La presente Política entrará en vigencia al momento de ser publicada. El contenido de este documento será revisado anualmente o cuando ocurran eventos significativos que requieran su revisión y/o modificación.

10.2 Vigencia

La presente Política entrará en vigencia al momento de ser publicada.