



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PROCESO: Seguridad de la Información

P - SEGINF

Versión 7

Página 1 de 4

1. PROPÓSITO

Declarar la postura Organizacional en materia de Seguridad de la Información y establecer lineamientos internos que rijan la operación del negocio.

2. ALCANCE

Esta política debe ser de cumplimiento de todos los empleados y contratistas de UCCORP. De igual forma UCCORP velará por el acatamiento o alineamiento de las políticas de seguridad de la información con proveedores, partners de negocio y todas las partes interesadas pertinentes.

3. RESPONSABLE

El responsable de Seguridad será el principal encargado de establecer y hacer cumplir las políticas de seguridad de la información de la organización. De igual forma el responsable de Seguridad, con el apoyo del Comité de SI, será el encargado de gestionar las políticas de seguridad de la información, en todo su ciclo de vida.

4. DESCRIPCIÓN GENERAL

Para UCCORP, la seguridad de la información es de vital importancia. La firma reconoce el valor de la gestión adecuada de la información como activo de la organización para el desarrollo de la estrategia del negocio.

UCCORP gestiona la Seguridad de sus activos de información, y la ciberseguridad de las Tecnologías de Información y Comunicaciones (TIC) que soportan la infraestructura de su operación. Para el cumplimiento de estos, se ha establecido un Sistema de Gestión de Seguridad de la Información (SGSI), el cual está conformado por políticas, manuales, procedimientos, estándares, plataforma tecnológica, estructura organizacional y mecanismos de verificación y control; y tiene como propósito garantizar que los riesgos de seguridad de la información y los riesgos de ciberseguridad sean conocidos, asumidos, gestionados y mitigados de forma documentada, estructurada, eficiente y adaptable a los cambios que se produzcan en el entorno y las tecnologías.

La Política General de Seguridad de la Información contiene elementos fundamentales dentro del SGSI puesto que contienen directrices que enmarcan la actuación de todos los empleados, proveedores, terceros y son la base para la definición de las políticas

Elaborado por: Responsable de Seguridad

Revisado por: Comité de SI

Aprobado por: Comité de SI

Información de USO PÚBLICO / Fecha de Aprobación: 30-05-2022



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PROCESO: Seguridad de la Información

P - SEGINF

Versión 7

Página 2 de 4

específicas que se encuentran documentadas y publicadas en el documento Desglose Política de Seguridad de la Información.

Por lo tanto, la dirección de UCCORP se **compromete** a:

- Cumplir con los requisitos aplicables a la Seguridad de la Información.
- Desarrollar, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.
- Cumplir con la protección de la confidencialidad, integridad y disponibilidad de la información que gestiona la organización, de acuerdo con las mejores prácticas del mercado a nivel internacional.

5. OBJETIVOS DEL SG-SI:

Las Políticas de Seguridad de la Información tienen por objetivo la protección de los activos de información que dependen o usan las tecnologías de la información y las comunicaciones en UCCORP.

Los objetivos de seguridad de la información son los siguientes:

1. Mantener una cultura en Seguridad de la Información sólida, con cimientos fuertes y sostenible en el tiempo.
2. Identificar y solucionar de manera adecuada los incidentes de seguridad de la Compañía.
3. Controlar la exposición de los riesgos en seguridad de la información en la Compañía.
4. Mejoramiento Continuo del SG-SI.

6. POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

UCCORP cuenta con un Sistema de Gestión de la Seguridad de la Información (SGSI) que apoya la adecuada gestión de riesgos. Dicho Sistema soporta la debida protección de la información a partir de los pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- Todo empleado y parte interesada desde sus funciones en UCCORP debe cumplir y acatar los mecanismos de seguridad de la información indicados en el SG-SI.
- UCCORP debe cumplir con el diseño y la implementación de soluciones de negocio que aseguran los principios de la seguridad de los activos de información.
- UCCORP debe identificar y valorar los riesgos de la información desde el punto de vista de seguridad y aceptar los niveles de riesgo conforme con los objetivos del negocio y de acuerdo con ello determina los mecanismos de protección adecuados.
- UCCORP desde las etapas iniciales de los proyectos, debe incluir la evaluación de aspectos relacionados con la Seguridad de la información siguiendo los lineamientos establecidos al respecto.

Elaborado por: Responsable de Seguridad

Revisado por: Comité de SI

Aprobado por: Comité de SI

Información de USO PÚBLICO / Fecha de Aprobación: 30-05-2022



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PROCESO: Seguridad de la Información

P - SEGINF

Versión 7

Página 3 de 4

- UCCORP debe implementar reglas de acceso para que la información se encuentre debidamente protegida.
- UCCORP debe implementar mecanismos para promover el buen uso de los recursos tecnológicos.
- Toda información creada, almacenada o transmitida utilizando los recursos de UCCORP es de propiedad y uso exclusivo de la empresa y debe ser utilizada para el propósito del negocio.
- UCCORP debe atender y gestionar los incidentes relacionados con la seguridad de la información y ciberseguridad de la empresa de manera que se mitigue el impacto en la información.
- UCCORP cuenta también con unas políticas específicas de seguridad de la información como complemento a los procesos de la organización estipuladas en el documento **“PR - DESPSI Desglose de la Política de Seguridad de UCCORP”**

El incumplimiento de esta Política estará enmarcado dentro del proceso disciplinario definido por UCCORP en su Reglamento Interno de Trabajo.

6. DOCUMENTOS Y REGISTROS RELACIONADOS

- Desglose Política de Seguridad de la Información

Elaborado por: Responsable de Seguridad

Revisado por: Comité de SI

Aprobado por: Comité de SI

Información de USO PÚBLICO / Fecha de Aprobación: 30-05-2022



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PROCESO: Seguridad de la Información

P - SEGINF

Versión 7

Página 4 de 4

7. CONTROL DE CAMBIOS

| FECHA REVISIÓN | VERSIÓN | DESCRIPCIÓN DEL CAMBIO | PARTICIPANTES |
|----------------|---------|--|--------------------------|
| Mayo 2018 | 1 | Creación del documento | Responsable de Seguridad |
| Junio 2019 | 2 | Se crea una segunda versión de las políticas para dar cumplimiento a los requisitos de la Norma ISO27001. | Responsable de Seguridad |
| Diciembre 2019 | 3 | Ajustes a la política para dar cumplimiento a la Cláusula 5.2 de la Norma ISO 27001. (Inclusión de los objetivos de SI, Roles, responsabilidades, enlace con otras políticas) | Responsable de Seguridad |
| Noviembre 2020 | 4 | Referenciar todas las políticas descritas en el desglose y asegurar el formato establecido. | Responsable de Seguridad |
| Enero 2021 | 5 | Ajuste de la descripción del compromiso de la empresa en proteger los atributos de la información y alineado con prácticas internacionales en general y ajuste en la enumeración de las políticas de detalle (desglose). | Responsable de Seguridad |
| Marzo 2021 | 6 | Se incluye en el punto 5. Descripción General, el compromiso de cumplir con los requisitos aplicables a la seguridad de la información. | Responsable de Seguridad |
| Mayo 2022 | 7 | Se reestructura toda la política para simplificar y detallar cada requisito de seguridad de la información | Responsable de Seguridad |

Elaborado por: Responsable de Seguridad

Revisado por: Comité de SI

Aprobado por: Comité de SI

Información de USO PÚBLICO / Fecha de Aprobación: 30-05-2022