



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Diciembre de 2019 – V3

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN



Detalle del cambio	Fecha/Versión del cambio	Realizado por (Dueño del documento)	Aprobado por
Creación del documento	Mayo 2018	Oficial de SI	Comité de SI – Acta 001 2019
Se crea una segunda versión de las políticas para dar cumplimiento a los requisitos de la Norma ISO27001.	Junio 2019	Oficial de SI	Comité de SI – Acta 004 2019
Ajustes a la política para dar cumplimiento a Cláusula 5.2 de la Norma ISO 27001. (Inclusion de los objetivos de SI, Roles, responsabilidades y autoridades, enlace con otras politicas)	Diciembre 2019	Oficial de SI	Comité de SI – Acta 003 2020



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Diciembre de 2019 – V3

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.

Por lo tanto, la dirección de UCCORP se compromete a desarrollar, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información que propenda por la mejora continua y evolución en la madurez de la gestión de la seguridad de su información, según el estándar ISO 27001:2015.

Para ello la compañía ha establecido los siguientes roles, responsabilidades, autoridades y Objetivos de Seguridad:

Oficial de Seguridad:

Apoya el negocio en la definición de la Estrategia y Objetivos de seguridad de la Información. Entre sus responsabilidades esta:

- Establece y apoya el mantenimiento del SGSI.
- Mantiene el ciclo de vida de la Política de Seguridad de la Información de la Compañía.
- Lidera las sesiones del Comité de SI.
- Vela por el cumplimiento de las Políticas de SI.
- Gestiona los recursos necesarios para la correcta operación del SGSI.
- Asegura que los Roles y Responsabilidades de Seguridad de la Información estén claramente establecidos en la Organización.
- Mantiene el programa de Formación y Sensibilización en SI.
- Apoya en la definición de procesos de SI.
- Apoya la gestión de incidentes de SI, según el proceso establecido.
- Mantiene actualizada y vigente los contactos con autoridades y entes regulatorios relacionados a la SI.



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Diciembre de 2019 – V3

Comité de Seguridad:

Conformado por Comité de Gerencia, el cual sesionará mínimo cada tres meses con temas relacionados a SI, o en cualquier otro momento que así lo requiera el Negocio. Entre sus responsabilidades esta:

- Establece los objetivos de Seguridad de la Información y hace seguimiento a su cumplimiento.
- Aprueba las Políticas de Seguridad de la Información.
- Aprueba políticas de detalle, como: Política de Directorio Activo, Política de respaldos, entre otros.
- Aprueba los planes de acción de SI y realiza seguimiento de éstos.
- Hace seguimiento a la efectividad de los controles de SI.
- Realiza la aprobación de los documentos que conforman el SGSI.
- Hace el seguimiento a los indicadores del SGSI.

Objetivos del SGSI – Uccorp:

Crear una cultura en Seguridad de la Información sólida, con cimientos fuertes y sostenible en el tiempo.

Mantener los incidentes de seguridad dentro de niveles aceptables. (Severidad Media o Baja).

Gestionar continuamente los riesgos de SI, promoviendo el constante monitoreo de nuevos riesgos que surjan, y de hacer seguimiento a los planes de acción.



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Diciembre de 2019 – V3

1. La seguridad de la Información es responsabilidad de todos: En UCCORP, todo funcionario o tercero que accede a la información de la organización debe velar por preservar la seguridad de la información a la que tiene acceso.
2. Todo individuo en la organización debe reportar al Oficial de seguridad, cualquier comportamiento violatorio identificado y que atente contra la seguridad de la información.
3. Todo individuo en la organización deberá identificar el riesgo de seguridad de la información en cualquier acción que emprenda y obrar de acuerdo a los procedimientos y políticas establecidas. Si no identifica la ruta de acción, deberá elevar la consulta al Oficial de seguridad.
4. Todos los empleados y partes externas cuando aplique, deberán acatar las siguientes políticas dispuestas en el desglose de este documento:
 - Política de Activos de Información, Clasificación y Etiquetado.
 - Política de dispositivos móviles y trabajo remoto
 - Manejo de Medios Removibles
 - Control de Acceso
 - Control de software no autorizado
 - Seguridad física del cuarto técnico
 - Seguridad en Oficinas.
 - Desarrollo Seguro
 - Seguridad en las comunicaciones
 - Política de Respaldos
 - Gestión de Vulnerabilidades

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