1. PROPÓSITO

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

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 o partners de negocio.

3. RESPONSABLE

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

4. DEFINICIONES

Activo de información

Un activo de información en el contexto de la norma ISO/IEC 27001 es: “algo que una organización valora y por lo tanto debe proteger”.
Se puede considerar como un activo de información:

- Los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios.
- El hardware y el software utilizado para el procesamiento, transporte o almacenamiento de información.
- Los servicios utilizados para la transmisión, recepción y control de la información.
- Las herramientas o utilidades para el desarrollo y soporte de los sistemas de información.
- Personas que manejen datos, o un conocimiento específico muy importante para la organización (Por ejemplo: secretos industriales, manejo de información crítica, know how).

Riesgo de Seguridad de la Información

Se refiere al impacto a la organización y a sus accionistas que pueda tener debido a amenazas y vulnerabilidades asociadas en la operación, el uso de los sistemas de información y el ambiente en los que éstos operan.

Potencial daño, dada una amenaza que explote una vulnerabilidad de un activo o grupo de activos y por tanto causar daño a la Organización.

Trabajo remoto

Consiste en realizar una actividad profesional a distancia. Se mantiene una relación empleado-empleador y las mismas responsabilidades que se obtendrían en un trabajo de oficina. De igual forma los empleados remotos suelen cumplir con un horario laboral al igual que lo harían en cualquier otro trabajo.

Dispositivos móviles

Tipo de computadora de tamaño pequeño, con capacidades de procesamiento, con conexión a Internet, con memoria, diseñado específicamente para una función, pero que pueden llevar a cabo otras funciones más generales.
Algunos tipos de dispositivos móviles son:
Teléfonos inteligentes y tabletas, agendas digitales, tarjetas inteligentes, entre otros dispositivos.

Medio removible
Dispositivos de almacenamiento independientes del computador que pueden ser trasportados libremente

Vulnerabilidad
Una vulnerabilidad, en el contexto del presente documento, es una debilidad o falla en un sistema de información que pone en riesgo la seguridad de la información, pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma. Estos «agujeros» pueden tener distintos orígenes por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos

5. 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.

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 contínua 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 y Objetivos de Seguridad:

Director 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.

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:

1. Crear una cultura en Seguridad de la Información sólida, con cimientos fuertes y sostenible en el tiempo.
2. Mantener los incidentes de seguridad dentro de niveles aceptables. (Severidad Media o Baja).
3. Gestionar continuamente los riesgos de SI, promoviendo el constante monitoreo de nuevos riesgos que surjan, y de hacer seguimiento a los planes de acción

Lineamientos Generales

- 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.
- Todo individuo en la organización debe reportar al Director de Seguridad, cualquier comportamiento violatorio identificado y que atente contra la seguridad de la información.
- 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 Director de Seguridad.
- Todos los empleados y partes externas cuando aplique, deberán acatar las siguientes políticas o lineamientos dispuestas en el desglose de este documento:

- Metodología de Riesgos de Seguridad de la Información
- Activos de Información, Clasificación y Etiquetado.
- Uso inaceptable de los activos de información
- Política de teletrabajo
- Política para dispositivos móviles
- Políticas de transferencia de información
- Manejo de Medios Removibles
- Gestión/Disposición de medios
- Seguridad de los Recursos Humanos
- Política de Control de Acceso
- Protección de contraseñas
- Mantenimiento de Equipos
- Control de software no autorizado
- Seguridad en área de trabajo
- Desarrollo Seguro
- Política de Respaldos
- Antivirus
- Gestión de Vulnerabilidades
- Política de Seguridad de la Información para las relaciones con proveedores
- Continuidad
- Política sobre el uso de controles criptográficos – En construcción
- Política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida – En construcción
- Política de escritorio y pantalla limpia
- Política de desarrollo seguro – En construcción

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

Mapa de Procesos
Listado Maestro de Documentos
Desglose Política de Seguridad de la Información

7. BIBLIOGRAFÍA

-Instituto Colombiano de Normas Técnicas y Certificación. Norma Técnica Colombiana NTC-ISO-27001

8. CONTROL DE CAMBIOS

FECHA REVISIÓN	VERSIÓN	DESCRIPCIÓN DEL CAMBIO	PARTICIPANTES
Mayo 2018	1	Creación del documento	Director de Seguridad
Junio 2019	2	Se crea una segunda versión de las políticas para dar cumplimiento a los requisitos de la Norma ISO27001.	Director de Seguridad
Diciembre 2019	3	Ajustes a la política para dar cumplimiento a Cláusula 5.2 de la Norma ISO 27001. (Inclusión de los objetivos de SI, Roles, responsabilidades, enlace con otras políticas)	Director de Seguridad
Noviembre 2020	4	Referenciar todas las políticas descritas en el desglose y asegurar el formato establecido.	Director de Seguridad