POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CORPALLANOS.

1. INTRODUCCIÓN

El presente manual hace parte integral de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.

Se tienen en cuenta las siguientes leyes y decretos:

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993 "por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944." (Derechos de autor).
- Ley 527 de 1999 "por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".
- Ley 594 de 2000 "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales".

2. TÉRMINOS Y DEFINICIONES

Con el objeto de precisar el alcance de los principales conceptos utilizados en este documento, se transcriben las definiciones:

- **Activo:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.
- **Activo crítico:** Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles.
- **Administración de Riesgos**: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

- **Análisis de Impacto al Negocio:** Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.
- **Áreas Seguras:** Son aquellas en donde se encuentren sistemas de procesamiento y almacenamiento informático o de datos.
- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Centro de cableado:** el centro de cableado es el lugar donde se ubican los recursos de comunicación de Tecnología de información, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos).
- **Ciberactivo:** Se identifica como foco de la ciberseguridad los activos digitales como datos, dispositivos y sistemas que permiten a la organización cumplir con sus objetivos de negocio.
- **Ciberseguridad:** Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
- **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Desastre Tecnológico:** Se define como una situación, derivada de un accidente en el que se involucran sustancias químicas peligrosas o equipos peligrosos; que causa daños al ambiente, a la salud, al componente socioeconómico y a la infraestructura, siendo estos daños de tal magnitud que exceden la capacidad de respuesta del componente del afectado.
- **Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- **Dispositivos móviles:** Equipo de cómputo pequeño, cuyo concepto principal es la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.
- **Equipos activos de red:** son todos los dispositivos que hacen la distribución de las comunicaciones a través de la red de datos.
- **Evaluación de Riesgos:** Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de esta, la probabilidad de que ocurran y su potencial impacto en la operación de la entidad.
- **Incidente de Seguridad:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o

audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Información Pública Clasificada:** "Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado…"
- **Información Pública Reservada:** "Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos…"
- **Paneles de conexión (patch panel):** Elemento encargado para la organización de conexiones en la red.
- **Propietario del riesgo:** Persona o proceso con responsabilidad y autoridad para gestionar un riesgo.
- **Protección a la duplicación:** Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **Responsable de Seguridad de la información:** Es la persona que cumple la función de supervisar el cumplimiento de la presente Política, coordinar el Comité de Seguridad de la Información y de asesorar en la materia a los integrantes de la entidad que así lo requieran.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- **Tecnologías de la Información:** Las tecnologías de la información y las Comunicaciones (TIC o TICs), Nuevas Tecnologías de la Información y de la Comunicación (NTIC), agrupan los elementos y las técnicas utilizadas en el
- tratamiento y la transmisión de las informaciones, principalmente de informática, internet y telecomunicaciones.

3. PARTES INTERESADAS

Las partes interesadas corresponden a las personas naturales o jurídicas con la cual CORPALLANOS interactúa en el ejercicio de sus funciones, que pueden afectar o ser afectadas por la Seguridad de la Información y en algunos casos, pueden manifestar un interés directo, explícito y comprometido con los objetivos y propósitos del Sistema de Gestión de Seguridad de la Información - SGSI.

4. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Organización interna: Dictar lineamientos que permitan administrar la seguridad de la información dentro CORPALLANOS y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades y poder aplicar las medidas de seguridad adecuadas en los accesos de terceros a la información de CORPALLANOS.

Política para dispositivos móviles: Establecer los lineamientos para el uso, administración, consulta y operación de los servicios en los dispositivos móviles de CORPALLANOS y a su vez controlar el acceso a los mismos, en las instalaciones de CORPALLANOS

Política para teletrabajo: Establecer los lineamientos en materia del Sistema de Gestión de Seguridad de la Información que tiene los colaboradores de CORPALLANOS. que se acogen a la modalidad de Teletrabajo para el uso, administración, consulta y operación de los servicios en las áreas de Teletrabajo.

5. SEGURIDAD DEL RECURSO HUMANO

CORPALLANOS deberá definir una lista de verificación que contengan los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo con lo que dicta la ley y la reglamentación vigente.

Los procesos de selección de personal de planta y procesos contractuales deberán contener la autorización para el tratamiento de los datos personales de acuerdo con la política de tratamiento de datos personales de CORPALLANOS y de acuerdo con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.

Términos y condiciones del empleo: Recursos humanos deberá definir los términos y condiciones del contrato, en los cuales se establecerá las obligaciones del contratista en materia de seguridad de la información, las leyes de propiedad intelectual, de protección de datos personales, de transparencia y acceso a la información pública.

Recursos Humanos deberá dar a conocer a los colaboradores los términos y condiciones de empleo o contrato y especificar las responsabilidades u obligaciones en materia de la seguridad de la información y aclarar que estas se extienden más allá de los límites de CORPALLANOS y del horario normal de trabajo o de ejecución del objeto contractual.

Recursos humanos deberán hacer firmar un documento de compromiso de confidencialidad de la información a los colaboradores, dicho documento debe reposar en la historia laboral o expediente contractual según sea el caso.

Proceso disciplinario: En lo pertinente al incumplimiento y desacato de las políticas de la seguridad de la información, se aplicará lo establecido en los procedimientos destinados para tal fin, por recursos humanos de CORPALLANOS.

6. GESTIÓN DE ACTIVOS

Inventario y propiedad de los activos: Los líderes de los procesos deberán mantener un inventario de sus activos de información de forma anual y serán actualizados según el evento en que se requiera.

Devolución de activos: Todos los colaboradores y terceras partes deberán devolver todos los activos de información de CORPALLANOS que se encuentren a su cargo al terminar su empleo, contrato o acuerdo.

7. CONTROL DE ACCESO

CORPALLANOS suministrará a los usuarios las credenciales respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, de esta forma las credenciales de acceso son de uso personal e intransferible.

Es responsabilidad de los colaboradores o terceras partes de CORPALLANOS el manejo que se les dé a las credenciales de acceso asignadas.

8. SEGURIDAD FÍSICA Y DEL ENTORNO

Controles de acceso físicos Seguridad de oficinas, recintos e instalaciones: CORPALLANOS dictará lineamientos para proteger a través de controles de acceso para que solo se permita el ingreso a personal autorizado a las áreas seguras.

Protección contra amenazas externas y ambientales: CORPALLANOS establecerá los lineamientos para los controles contra amenazas externas y ambientales y quedarán enmarcadas en los planes de contingencia, de emergencia y de continuidad de la operación.

Ubicación y protección de los equipos: Los equipos de cómputo e impresoras deberán estar situados y protegidos para reducir el riesgo contra amenazas ambientales y de acceso no autorizado. Los equipos de cómputo portátiles se deberán proteger mediante mecanismos que no permitan su pérdida.

Mantenimiento de equipos: Las actividades de mantenimiento tanto preventivo como correctivo deberán registrarse. Solo el personal autorizado deberá llevar a cabo el mantenimiento o las reparaciones a los equipos.
Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deberán ser programadas.

Instalación de software en sistemas operativos: CORPALLANOS deberá controlar y tener registros de la actualización del software en producción, aplicaciones y librerías de programas propios de CORPALLANOS.

Restricciones sobre la instalación de Software: CORPALLANOS deberá controlar la instalación y uso de máquinas virtuales y sólo podrá realizarse siempre y cuando sea una necesidad para el uso de las funciones o labor contratada y no viole derechos de autor.

Acuerdos de confidencialidad o de no divulgación: Se deberán identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

9. RELACIÓN CON PROVEEDORES.

Política de seguridad de la información para las relaciones con proveedores: La Dirección de Contratación deberá establecer lineamientos para el cumplimiento de las obligaciones contractuales del Eje de Seguridad de la Información con terceros o proveedores.

La Dirección de Contratación deberá establecer en el momento de suscribirse contratos de apoyo a la gestión que se desarrollen dentro de

CORPALLANOS, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información de CORPALLANOS.

10. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

CORPALLANOS Dictar lineamientos que permitan asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

.