|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Logo Empresa | **MANUAL DE SEGURIDAD INFORMÁTICA** | **Código** | TI-SEG-01 | |
| **Fecha** | 10 de sept. de 2019 | |
| **Versión** | 1 | Pagina 1 de 7 |

Tabla de contenido

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Introducción | | 2 |
| 2. | Objetivo | | 3 |
| 3. | Alcance | | 3 |
| 4. | Definiciones | | 4 |
| 5. | Descripcion de controles | | 5 |
|  | 5.1 | Controles Generales | 6 |
|  | 5.2 | Controles especifícos | 6 |
|  | 5.3 | Criterios de la información | 7 |
|  | 5.4 | Controles referentes a la seguridad | 7 |

1. **INTRODUCCIÓN**

Este documento describe la normas de seguridad de la información definidas por la empresa.

La normas incluidad en este documento se constituyen parte integral del sistema de gestión y de seguridad de la información de la compañía. Y se convierte en base para la implementación de los controles, procedimientos y estandares definidos.

Tambien atiende a actividad III de curso virtual de Seguridad y Redes, impartido por el sistema nacional de aprendizaje (SENA).

La seguridad de la información es una prioridad para la compañía y por lo tanto es resposabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de estas normas.

1. **OBJETIVO**

Establecer las normas de seguridad de la información de la compañía, con el fin de regulas la gestión de la seguridad de la información al interior de la empresa.

1. **ALCANCE**

Las normas de seguridad de la información cubren todos los aspectos administrativos y de control que deber ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación con la empresa, para conseguir un adecuado nivel de protección de las características de seguridad de la información.

1. **DEFINICIONES**

Activo de información: Cualquier componente (humano, tecnológico, software, infraestructura, documentación) que soporta uno o mas procesos de negocio de la compañía y que en consecuencia debe ser protegido.

Acuerdo de Confidencialidad: Es el documento en el que los funcionarios, o proveedores o provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la compañía, comprometiéndose a no divulgar, usar o explotar la información a la que tenga acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de Riesgo de la seguridad de la información: Proceso sistemático de identificación de fuentes, estimación de impactos, probabilidades y comparación de dichas variables contra criterio de valuación para determinar las consecuencias potenciales de pérdida de confidencialidad de la información.

Autenticación: El proceso de comprobación de identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Capacity Planing: Proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

Centro de Computo: Es la zona o espacio designado para el almacenamiento de computadores (servidores) para un fin especifico, los cuales se encuentran conectados entre si a través de una red de datos, el Centro de datos debe cumplir con estándares, con el fin de garantizar los controles de acceso físicos, los materiales de paredes, pisos y techos, el suministro de alimentación o fluido eléctrico y las condiciones medioambientales de temperatura y humedad adecuados.

Centros de Cableado: Son las habitaciones o espacios designados donde se deberán instalar los dispositivos de comunicación y de cableado estructurado, al igual que los centros de computo, los centros de cableado deben cumplir requisitos mínimos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación o fluido eléctrico y condiciones de temperatura y humedad.

Cifrado: La transformación de los datos mediante el uso de la criptografía para producir datos inteligibles (cifrados) y asegurar su confidencialidad, este cifrado es muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: Asegurar que los accesos a sistemas de información y sus recursos relacionados sean solo realizados por los funcionarios de la empresa, basados en la necesidad de saber o de hacer de sus cargos. Garantizando que la información no este disponible o divulgada a personas o procesos no autorizados.

Control: Toda actividad o proceso encaminado a mitigar o evitar un riesgo, incluye políticas, procedimientos, guías, estructuras organizacionales y buenas practicas, que puedan ser de carácter administrativo, tecnológico, físico o legal.

Custodio del Activo de Información: La unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Integridad: Proteger la exactitud y plenitud de los sistemas de información y sus recursos relacionados, limitando la gestión sobre los mismos a personas autorizadas y programas de aplicación aprobados y autorizados, protegiéndolos contra pérdida, destrucción o modificaciones accidentales o intencionales.

Disponibilidad: Asegurar que los usuarios autorizados tienen acceso a los sistemas de información y sus recursos relacionados, en tiempo y forma, cuando sean requeridos.

Privacidad: Criterio de la información para evitar que trascienda a terceras personas información de propiedad de la empresa, referida a individuos, protegiendo a los mismos contra la divulgación indebida de su información personal y protegiendo la responsabilidad de la empresa sobre este tipo de divulgaciones.

Vulnerabilidad: Las debilidades que la organización presenta frente a alguna eventual amenaza.

Amenaza: Conjunto de peligros a los que están expuestos los sistemas de información y sus  recursos tecnológicos relacionados.

Incidente de Seguridad: Un evento adverso, confirmado o bajo sospecha que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, plataforma tecnológica, la frecuencia, las consecuencias, el numero de veces ocurrido o el origen (interno o externo).

Inventario de Activos de información: Lista ordenada y documentada de los activos de información pertenecientes a la compañía.

Licencia de software: Contrato en donde se especifican todas las normas y clausulas que rigen el uso de un determinado producto de software, teniendo en cuenta alcances de uso, instalación, reproducción y copia de estos productos.

Medios removibles: Cualquier componente extraíble de hardware que sea usado para el almacenamiento; los medios removibles incluyen cintas, discos duros removibles, unidades de almacenamiento USB, CDs, DVDs, entre otros.

Propietario de Información: La unidad organizacional o proceso donde se crean los activos de información.

Recursos Tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y servicios de red), estaciones de trabajo, equipos portátiles, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento del trabajo al interior de la empresa.

Responsable por el Activo de Información: Persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y la disponibilidad de los activos de información, es decir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

Eficacia: característica de la información que indica que debe ser relevante y pertinente para los procesos de la organización, así como entregarse oportunamente y en forma correcta, coherente y completa, que pueda utilizarse.

Conformidad: Cumplimiento de las leyes, reglamentaciones y obligaciones contractuales a la que están sujetos los procesos de la organización, es decir, criterios de gestión, impuestos desde fuera de la misma.

Responsabilidad: Los sistemas deben brindar una información apropiada a los niveles de decisión para su utilización en la operación de la organización y en la entrega de información a los organismos regulatorios con respecto al cumplimiento de las leyes y reglamentaciones.

Terceros: Todas las personas jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la Compañía.

1. **DESCRIPCIÓN DE CONTROLES SOBRE LA SEGURIDAD.**
   1. **CONTROLES GENERALES.**

Los controles generales representan los procedimientos de control interno establecidos por la empresa, para asegurar que el uso de las tecnologías de la información se desarrollen de acuerdo a lo esperado. Los controles generales se han direccionado al control de los procesos informáticos que se pueden agrupar en dos grandes categorías:

* **Procesos informáticos básicos:** Son los procesos que tienen relación directa con los servicios que se prestan a los usuarios de los sistemas de información y sus tecnologías relacionadas. Estos procesos consisten en tomar un insumo, agregarle valor y generar un producto que satisface a un cliente interno o externo. Normalmente estos procesos son repetitivos y están conformados por los siguientes elementos: proveedor, insumo, proceso, producto y cliente.

Los principales procesos informáticos básicos con los siguientes:

* Mantenimiento de Sistemas.
* Integración de paquetes de software.
* Capacitación.
* Procesos de datos en ambientes de trabajo en lote.
* Atención a requerimientos de usuarios.
* Administración de procesos especiales.
* **Procesos de Administración Informática:** Son procesos necesarios para el funcionamiento del área de servicios informáticos, que debe administrar los recursos a su cargo. Normalmente estos procesos no son repetitivos o sus ciclos son más largos. Los principales procesos de administración informática son:
* Planeación estratégica de tecnología.
* Dirección y control del área de tecnología.
* Administración de recursos materiales.
* Administración de recursos humanos.
* Administración de recursos financieros.
  1. **CONTROLES ESPECÍFICOS.**

Los controles específicos o controles de las aplicaciones constituyen los procedimientos de control interno y externo, establecidos por la empresa para el cumplimiento de los objetivos para los que fueron creados estos procesos, incluyendo los siguientes:

* Ingreso de datos.
* Comunicación de datos.
* Procesamiento de datos.
* Salida y distribución de datos e informes.
* Accesos.
* Continuidad del sistema.

Si no se explican los controles definidos precedentemente, los activos informáticos quedarían expuestos al acceso y manejo por parte de personas no autorizadas.

* 1. **CRITERIOS DE LA INFORMACIÓN.**

En cuanto a la información proporcionada por los sistemas y de acuerdo con los estándares generalmente aceptados, en la empresa los estándares establecidos deben reunir los criterios de eficiencia, confiabilidad, integridad, disponibilidad, cumplimiento y contabilidad.

* 1. **CONTROLES REFERENTES A LA SEGURIDAD.**

Dentro de estos controles se distinguen 3 grupos generales relacionados a seguridad

* + 1. **Controles sobre seguridad física**

Permite proteger los recursos de integran los sistemas informáticos contra amenazas físicas accidentales o intencionales.

* + 1. **Controles sobre Seguridad Lógica**

Permite proteger los datos y sistemas, de accesos y manipulaciones no autorizadas

* + 1. **Controles sobre Seguridad Legal**

Son los controles que se implementan en la compañía para proteger a la organización con respecto a asuntos de propiedad del software, contrataciones de servicios y sistemas informáticos, relación con el personal, uso de correos electrónicos, uso de Internet y similares.

Para la empresa resulta de la mayor importancia asegurar que todos los aspectos de la organización están de conformidad a los marcos legales aplicables. Por consiguiente, para todos los efectos de asuntos relativos a la Seguridad Legal, la empresa no habilita ningún uso, aplicación, servicio o herramienta que no se encuentre autorizada de forma expresa, y requiere de sus empleados el ceñimiento estricto a esta disposición.