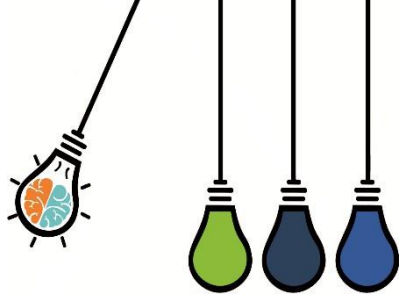
Formación

Consultores Legales AB

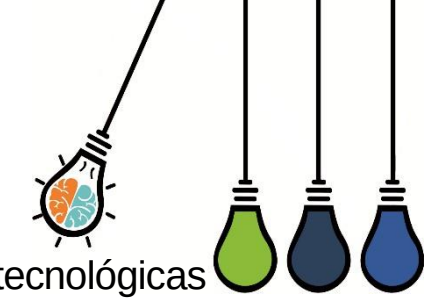
Dirección de Tecnología

POLITICA DE SEGURIDAD DE LA INFORMACION



- Concepto General.
- Objetivos.
- Características de la Información.
- Funciones y Responsabilidades.
- Clasificación de la Información.
- Control de Acceso.
- Política de Escritorio y Pantalla Limpia.
- Incidentes de Seguridad.

CONCEPTO GENERAL



La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información. Estos riesgos que se enfrentan han llevado a que se desarrolle un documento de directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

En este sentido, las políticas de seguridad informática definidas partiendo desde el análisis de los riesgos a los que se encuentra propensa **CONSULTORES LEGALES AB**, surgen como una herramienta organizacional para concienciar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer nuestra política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades en su aplicación, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea a **CONSULTORES LEGALES AB.**

OBJETIVO

Desarrollar un sistema de seguridad significa "planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la empresa".

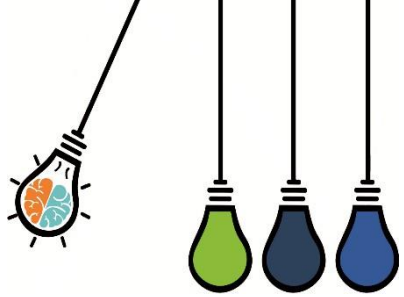
Los objetivos que se desean alcanzar luego de implantar nuestro sistema de seguridad son los siguientes:

Proteger, preservar y administrar objetivamente la información de **CONSULTORES LEGALES AB**, junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad y disponibilidad de la información.

Compromiso de todo el personal de la empresa con el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.

Todos los empleados se convierten en interventores del sistema de seguridad.

CIRCULARES EXTERNAS SIFC



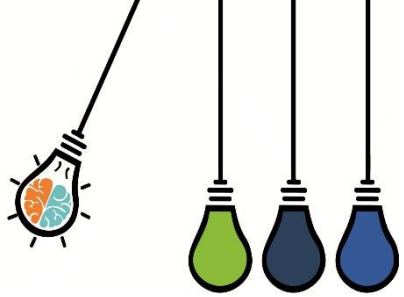
CIRCULAR 048 DE 2008

Síntesis: La reglamentación no define lo que se considera “horarios adecuados” para que las entidades vigiladas adelanten su gestión de cobranza para la recuperación de cartera morosa toda vez que no se trata de imponer un determinado horario para su desarrollo pues una previsión de tal naturaleza podría llegar a ser inoperante. Cada actividad adelantada para la gestión de cobranza dependerá del perfil del cliente y deberá quedar registrada en el historial del deudor.

Gestión de Cobranzas: en relación con las **condiciones de la gestión de cobranza para la recuperación de cartera morosa.** En efecto, el objeto de la citada Circular es garantizar que las entidades vigiladas actúen dentro del marco general de la debida diligencia en la prestación del servicio -a la que están obligadas legalmente en virtud de la previsión contenida en el numeral 4.1. del artículo 98 del Estatuto Orgánico del Sistema Financiero-, en la gestión de cobranza a sus deudores morosos, de manera que se garanticen los derechos de los consumidores financieros.

- La labor debe adelantarse con profesionalismo, buen trato, respeto por el consumidor financiero y en horarios adecuados.
- Al momento del cobro se debe suministrar al deudor información cierta, suficiente, actualizada y de fácil comprensión, sobre el monto de la obligación, saldo pendiente, interés corriente y de mora, fechas de vencimiento y de pago, días de mora, datos de contacto de los funcionarios o terceros autorizados por la entidad vigilada a quienes puede acudir para realizar eventuales acuerdos de pago y la discriminación del orden en el cual se aplicará el pago que realizará el deudor (monto destinado a cubrir gastos de cobranza, intereses de mora, intereses corrientes y capital).
- Únicamente podrán ser trasladados los gastos de cobranza al deudor cuando se verifique que la entidad desplegó una actividad real encaminada a la recuperación de la cartera, el monto es razonable y proporcional a la gestión, se encuentran debidamente sustentado y ha sido previamente informado al consumidor financiero.
- Se considerará práctica no autorizada el cobro a los deudores por concepto gastos de cobranza en forma automática.

CIRCULARES EXTERNAS SIFC

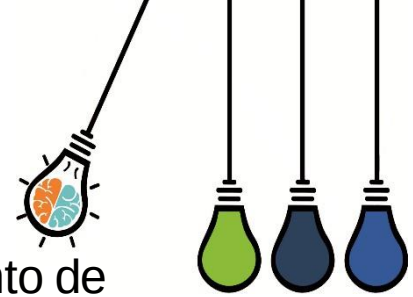


CIRCULAR 052 DE 2007

3.2. Tercerización – Outsourcing Las entidades que contraten bajo la modalidad de outsourcing o tercerización, a personas naturales o jurídicas, para la atención parcial o total de los distintos canales o de los dispositivos usados en ellos, o que en desarrollo de su actividad tengan acceso a información confidencial de la entidad o de sus clientes, deberán cumplir, como mínimo, con los siguientes requerimientos: 3.2.1. Definir los criterios y procedimientos a partir de los cuales se seleccionarán los terceros y los servicios que serán atendidos por ellos. 3.2.2. Incluir en los contratos que se celebren con terceros o en aquellos que se prorroguen a partir de la entrada en vigencia del presente Capitulo, por lo menos, los siguientes aspectos:

a) Niveles de servicio yoperación.
b) cuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas.
c) Propiedad de lainformación.
d) Restricciones sobre el software empleado.
e) Normas de seguridad informática y física a ser aplicadas.
f) Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de equipos o información.
g) Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.

CARACTERISTICAS DE LAINFORMACION



La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

Confidencialidad: Los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.

Integridad: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.

Disponibilidad: Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

FUNCIONES Y RESPONSABILIDADES

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de **CONSULTORES LEGALES AB,** cualquiera sea su situación contractual, el departamento al cual se encuentre vinculado y el nivel de las tareas que desempeñe.

La Junta Directiva aprueba esta Política y es la responsable de la autorización a sus modificaciones.

El Comité de Seguridad de la Información de la compañía es responsable de revisar y proponer a las directivas institucionales para su aprobación, el texto de la Política de Seguridad de la Información

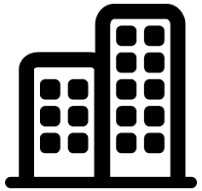
El Oficial de Seguridad de la Información será el responsable de coordinar las acciones del Comité de Seguridad de la Información

Los usuarios de la información y de los sistemas utilizados para su procesamiento, son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

CLASIFICACION DE LA INFORMACION

La información de **CONSULTORES LEGALES AB** será clasificada en 4 clases: Información Privilegiada, Información de Uso Interno, Información Confidencial e Información Pública. La información se encontrara clasificada en el encabezado del documento y por medio de marca de agua en el documento cuando serequiera.

Información Privilegiada: Es la Información a la que, por sus características, tienen acceso pocas personas, o lo tienen antes que otras muchas a las que también debe llegar.

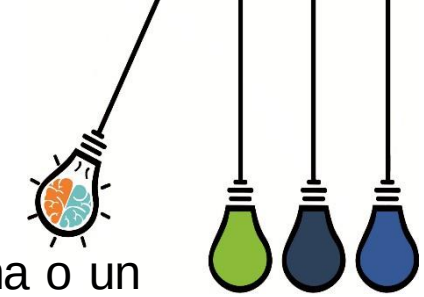


Información de Uso Interno: Se clasifica como información de Uso interno, aquella cuya revelación comporta riesgos para la entidad e incluye información estratégica, táctica u operativa.

Información Confidencial: Toda información que deba tratarse con confidencialidad será clasificada como Confidencial y se debe garantizar su protección con el fin de que no sea divulgada sin consentimiento de la persona.

Información Publica: Es la información que toda persona tiene derecho a manifestar por medio de la libertad de expresión y difusión de pensamiento oral o escrito, por cualquier medio de comunicación, sin previa autorización, sin censura o impedimento, siguiendo los reglamentos de la ley.

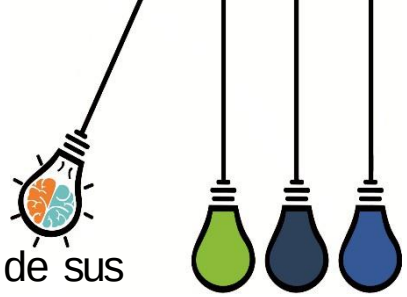
CONTROL DE ACCESO



El control de acceso consiste en la verificación de si un usuario, que puede ser una persona o un ordenador; que solicite acceso a un recurso, tiene los derechos necesarios para hacerlo. Un control de acceso ofrece la posibilidad de acceder a recursos físicos o lógicos.

La definición más generalizada de un control de acceso hace referencia al mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos. Básicamente encontramos controles de acceso en múltiples formas y para diversas aplicaciones. Por ejemplo, encontramos controles de acceso por software cuando digitamos nuestra contraseña para abrir el correo, otro ejemplo es cuando debemos colocar nuestra huella en un lector para encender el PC.

POLITICA DE ESCRITORIO Y PANTALLA LIMPIA



La política de escritorio limpio y pantalla limpia, permite la protección de la información en cualquiera de sus clasificaciones y que pueda estar contenida en escritorios, estaciones de trabajo, computadores portátiles, medio ópticos, medios magnéticos, documentos en papel y en general cualquier tipo de información que es utilizada para apoyar la realización de sus actividades en **CONSULTORES LEGALES AB**.

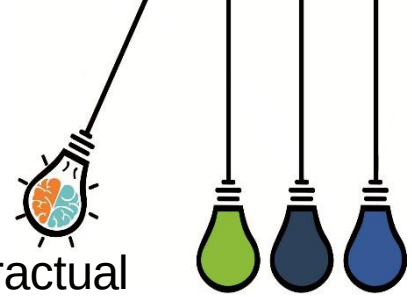
Los lugares de trabajo de todos los colaboradores, deben localizarse en ubicaciones que no queden expuestas al acceso de personas externas. De esta forma se protege tanto los equipos tecnológicos, como lo documentos que pueda estar utilizando el usuario. Los equipos que queden ubicados cerca de zonas de atención o tránsito de público, deben situarse de forma que las pantallas no puedan ser visualizadas por personas externas.

Todos los usuarios deben cumplir las normas de escritorio limpio descritas a continuación:
Está prohibido contar con elementos como esferos o lápices, que permitan copiar información confidencial; del mismo modo se prohíbe el uso de papel en las estaciones de trabajo de los asesores de cobranzas.

Se encuentra prohibido el ingreso de celulares, memorias USB o dispositivos de almacenamiento, a las áreas de operación.

Si el perfil de usuario le permite el manejo de documentos físicos en su estación de trabajo, estas deben estar bajo llave en ausencia del responsable y al final de la jornada de trabajo debe guardar en un lugar seguro los documentos que contengan información confidencial.

INCIDENTES DE SEGURIDAD

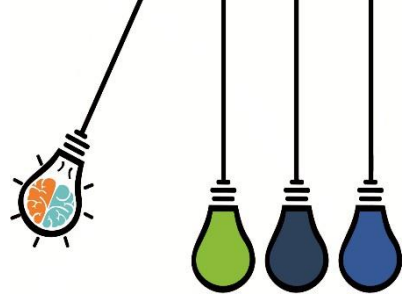


El personal de **CONSULTORES LEGALES AB** o cualquier tercero sin importar su situación contractual debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su Supervisor inmediato. En casos especiales dichos reportes podrán realizarse directamente a la Dirección Administrativa, la cual debe garantizar las herramientas informáticas para que formalmente se realicen tales denuncias.

El Comité de Seguridad de la Información debe preparar, mantener y difundir las normas, procesos y guías para el reporte e investigación de incidentes de seguridad.

Como norma general el empleado que viole alguna de las disposiciones antes mencionadas en relación con lo que se considera objeto de la Confidencialidad, o se evidencie violación alguna a las diferentes normas establecidas y en general que su acción deba ser considerada como un riesgo para la compañía, será objeto de evaluación. En todo caso en comité designado, se determinara el tipo de culpa o dolo, dimensionando todos los riesgos implícitos, internos y externos, determinando con precisión las acciones que se deban tomar para la corrección y por consiguiente el tipo de sanción a que haya lugar.

Gracias.....



Consultores Legales AB

A&B
Consultores legales