Política de Seguridad de la Información

Generalidades

La información es uno de los recursos más valioso para la empresa y por lo tanto debe ser protegida debidamente con los altos estándares de seguridad

El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la empresa apoyadas en un correcto sistema de información.

La empresa establecerá los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la presente política como de los demás componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas de gestión.

Alcance

Esta política es de aplicación en el conjunto de dependencias que componen la empresa, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la organización a través de contratos o acuerdos con terceros y a todo el personal de la empresa, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

Objetivos

- Proteger, preservar y administrar objetivamente la información de la empresa y sus afiliados, junto con las tecnologías utilizada 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, disponibilidad, legalidad, confiabilidad y no repudio de la información.
- Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de la empresa para asegurar su permanencia y nivel de eficacia.
- Definir las directrices de la organización para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

Responsabilidad

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la empresa, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe. Los directivos aprueban esta Política y son responsables de la autorización de sus modificaciones.

El Comité de Seguridad de la Información de la empresa es responsable de revisar y proponer a las directivas para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la organización. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la Empresa.

El Coordinador del Comité de Seguridad de la Información será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

El grupo responsable de Seguridad Informática será responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la operación del SGSI y supervisión del cumplimiento, dentro de la dependencia, de aspectos inherentes a los temas tratados en la presente Política.

El nivel de supervisión que pueda realizar cada grupo responsable de seguridad, está relacionado con el talento humano que lo conforma y en todo caso deberá ser aprobado por el Comité de Seguridad de la Información.

Los propietarios de activos de información son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

El jefe de Recursos Humanos cumplirá la función de notificar a todo el personal que se vincula contractualmente con la empresa, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los Compromisos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el 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.

La Oficina de Control Interno es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

Identificación, clasificación y valoración de activos de información.

Cada dependencia, bajo supervisión del Comité de Seguridad de la Información, debe elaborar y mantener un inventario de los activos de información que poseen (procesada y producida). Las características del inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el Comité de Seguridad de la Información, correspondiendo a la Oficina Asesora de Sistemas brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

Responsabilidades del personal de la Empresa

Todo el personal de la empresa, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información empresarial.

Los procedimientos para obtener tales perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada dependencia, de acuerdo a los lineamientos dados por la Oficina Asesora de sistemas, en cuanto a la información y la Red de Datos, en cuanto a los dispositivos hardware y los elementos software.

La empresa contempla procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones. La Oficina de Recursos Humanos junto con la Oficina Asesora de Sistemas se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

La Oficina Asesora de Sistemas se encargará de crear y mantener un centro documental de acceso general con información relacionada con temas de seguridad de la información tales como responsabilidad en la administración de archivos, buenas prácticas, amenazas de seguridad, entre otros.

Seguridad Física y del entorno

Acceso

Se debe tener acceso controlado y restringido a los cuartos de servidores principales, subsidiarios y a los cuartos de comunicaciones. Las empresas en conjunto con la Oficina Asesora de Sistemas laborarán y mantendrán las normas, controles y registros de acceso a dichas áreas.

Seguridad en los equipos

Los servidores que contengan información deben ser mantenidos en un ambiente seguro y protegido por los menos con:

- Controles de acceso y seguridad física.
- Detección de incendio y sistemas de extinción de conflagraciones.
- Bajo riesgo de inundación.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Toda información empresarial en formato digital debe ser mantenida en servidores aprobados por la Oficina Asesora de Sistemas. El Comité de seguridad define el límite de responsabilidades de las dependencias. No se permite el alojamiento de información empresarial en servidores externos sin que medie una aprobación por escrito del Comité de Seguridad de la Información.

La empresa debe asegurar que la infraestructura de servicios de TI este cubierta por mantenimiento y soporte adecuados de hardware y software.

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la empresa el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información empresarial.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares que para tal efecto elabore y mantenga el Comité de Seguridad en la Información.

Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad.

Administración de las comunicaciones y operaciones

Reporte e investigación de incidentes de seguridad

El personal de la empresa debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su jefe de dependencia. En casos especiales dichos reportes podrán realizarse directamente a la gerencia, 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.

En conformidad con la ley, la empresa podrá interceptar o realizar seguimiento a las comunicaciones por diferentes mecanismos y en todo caso notificando previamente a los afectados por esta decisión.

La empresa mantendrá procedimientos escritos para la operación de sistemas cuya no disponibilidad suponga un impacto alto en el desarrollo normal de actividades. A dichos sistemas se debe realizar seguimiento continuo del desempeño para asegurar la confiabilidad del servicio que prestan.

Pruebas de Vulnerabilidad

La empresa de verá ejecutar de manera periódica un análisis de pruebas de vulnerabilidad a sus equipos y sistemas y ejecutar controles para los riesgos identificados. Esta bajo la responsabilidad organizacional la contratación de una empresa competente que realice estas pruebas y defina las acciones a tomar frente a los riesgos identificados, en caso que el análisis se realice por personal interno, este deberá reportar a la dirección las acciones a tomar por escrito.

Protección contra software malicioso y hacking.

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multi-nivel que involucre controles humanos, físicos técnicos y administrativos. El Comité de Seguridad de la Información elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

En todo caso y como control mínimo, las estaciones de trabajo de la empresa deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de las estaciones no están autorizados a deshabilitar este control.

La empresa podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño. La dependencia que realice dicho seguimiento deberá informar a los funcionarios a través de correo electrónico o noticias en el portal empresarial de la ejecución de esta tarea.

La empresa debe mantener actualizada una base de datos con alertas de seguridad reportadas por organismos competentes y actuar en conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas informáticos.

Copias de Seguridad y Continuidad del Negocio

Toda información que pertenezca a la matriz de activos de información empresarial o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin. La Oficina Asesora de Sistemas debe proveer las herramientas para que las dependencias puedan administra la información y registros de copias de seguridad. La Oficina de Control Interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

Las copias de seguridad de información crítica deben ser mantenidas de acuerdo a cronogramas definidos y publicados, con el fin de garantizar su confidencialidad.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios. Los usuarios deben entregar al respectivo jefe de dependencia las copias de seguridad para su registro y custodia.

Administración de Configuraciones de Red

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida la empresa.

Todo equipo de TI debe ser revisado, registrado y aprobado por la empresa antes de conectarse a cualquier nodo de la Red de comunicaciones y datos empresariales.

Intercambio de Información con Organizaciones Externas

Las peticiones de información por parte de entes externos de control deben ser aprobadas por el área Administrativa y Financiera, y dirigida por dichos entes a los responsables de su custodia.

Internet y Correo Electrónico

Las normas de uso de Internet y de los servicios de correo electrónico serán elaboradas, mantenidas y actualizadas por el Comité de Seguridad de la Información y en todo caso este comité debe velar por el cumplimiento del código de ética empresarial y el manejo responsable de los recursos de tecnologías de la información.

Los funcionarios con acceso a información sensible no tendrán habilitados sistemas de información como correos electrónicos o internet, así como acceso a puertos de descarga como CD o USB, sin previa autorización de la gerencia.

Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas de la empresa deben ser aprobadas por el área de seguridad, de acuerdo a los procedimientos elaborados para tal fin por dichas dependencias.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. La empresa debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad que debe ser investigado.

Corresponde a la empresa mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos organizacionales.

Control de Acceso

Categorías de Acceso

Los accesos a los recursos de tecnologías de información deben estar restringidos según los perfiles de usuario definidos por el Comité de Seguridad de la Información.

Control de Claves y Nombres de Usuario

El acceso a información restringida debe estar controlado. Se recomienda el uso de sistemas automatizados de autenticación que manejen credenciales o firmas digitales.
Corresponde a la empresa elaborar, mantener y publicar los documentos de servicios de red que ofrece la organización a su personal.

La empresa debe elaborar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red. El acceso a sistemas de cómputo y los datos que contienen es responsabilidad exclusiva del personal encargado de tales sistemas. La empresa debe propender por mantener al mínimo la cantidad de cuentas de usuario que el personal debe poseer para acceder a los servicios de red.

El control de las contraseñas de red y uso de equipos es responsabilidad de la empresa. Dichas contraseñas deben ser codificadas y almacenadas de forma segura.

Las claves de administrador de los sistemas deben ser conservadas por la dirección de la empresa y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie. Se exceptúa de lo anterior las claves de administrador de servidores y equipos de escritorio adscritos a la Oficina Asesora de Sistemas las cuales deben ser conservadas por la Jefatura de la Oficina Asesora de Sistemas y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

La empresa en coordinación con la Oficina Asesora de Sistemas, deben elaborar, mantener y actualizar el procedimiento y las guías para la correcta definición, uso y complejidad de claves de usuario.

Como requisito para la terminación de relación contractual - o laboral - del personal de la empresa, la organización debe expedir un certificado de cancelación de las cuentas de usuario asignadas para el uso de recursos de tecnologías de la información de la empresa.

Auditoria y Seguimiento

Todo uso que se haga de los recursos de tecnologías de la información en la empresa deben ser seguidos y auditados de acuerdo con los lineamientos del Código de Ética y del Código de Uso de Recursos de Tecnologías de la Información, el cual debe ser elaborado por el Comité de Seguridad de la Información.
Acceso Remoto

El acceso remoto a servicios de red ofrecidos por la empresa debe estar sujeto a medidas de control definidas por la organización, las cuales deben incluir acuerdos escritos de seguridad de la información.

Control de elementos

Todo el personal de áreas sensibles de la organización está obligado a dejar elementos personales como celulares, morrales, cuadernos o cualquier otro elemento que pueda ser utilizado para la sustracción de información sensible de las plataformas de la empresa, en caso de evidenciarse incumplimiento a este ítem la organización podrá iniciar una investigación interna y tomar las medidas judiciales que apliquen en caso de evidenciarse actividades no permitidas o ilegales.

Adquisición, Desarrollo y Mantenimiento de Sistemas Software

Para apoyar los procesos operativos y estratégicos la empresa debe hacer uso intensivo de las Tecnologías de la Información y las Comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal propio.

La Oficina Asesora de Sistemas debe elegir, elaborar, mantener y difundir el "Método de Desarrollo de Sistemas Software en la organización" que incluya lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

Todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos del proyecto. La empresa no debe emprender procesos de desarrollo – o mantenimiento – de sistemas software que tengan asociados riesgos altos no mitigados.

Los sistemas software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.

Cumplimiento

Todo uso y seguimiento de uso a los recursos de TI en la empresa debe estar de acuerdo a las normas y estatutos internos, así como a la legislación nacional en la materia, incluido, pero no restringido a:

- Constitución Política de Colombia
- Ley 527-1999 Ley de comercio electrónico.
- NTC 27001:2006. Sistema de Gestión de Seguridad de la Información.
- PCI DSS (Payment Card Industry Data Security Standard)