POLÍTICA GENERAL DE SEGURIDAD Y CIBERSEGURIDAD DE LA INFORMACIÓN

OBJETIVO

El objetivo de esta política es establecer las pautas y mejores prácticas para proteger la información, los sistemas y la infraestructura de tecnología de la información de SETRACOL LTDA, contra amenazas cibernéticas. Esta política define las responsabilidades de los directivos, empleados y demás actores que intervienen en el manejo de la información.

Establecer las directrices de seguridad de la información digital y física, determinando las medidas para mantener su confidencialidad, su disponibilidad e integridad, la protección de los activos de información y la continuidad de los sistemas hacen parte de la organización.
La política de seguridad de la información contiene aquellos aspectos claves que se deben tener en cuenta para un adecuado uso de las tecnologías que posee la empresa con el fin de garantizar un manejo seguro y eficiente de estas.

ALCANCE

Esta política se aplica a todos los empleados, contratistas, proveedores y cualquier persona que acceda a los recursos de tecnología de la información de SETRACOL LTDA.

POLÍTICA DE CONFIDENCIALIDAD DE LA INFORMACIÓN

1. Independiente del medio en que se maneje ya sea escrito o verbal, el sistema de información tendrá el carácter de confidencial; toda la información operativa, administrativa y toda aquella que expresamente sea oficializada por los directivos.
2. Incurrirán en sanciones de tipo administrativo y penal, los empleados que sean sorprendidos o que se les compruebe uso inadecuado e Inapropiado de la información, o hayan manipulado información con el fin de confundir y ocultar situaciones que puedan afectar negativamente a la empresa.
3. Es responsabilidad de todos los empleados velar por la seguridad de la información de la compañía, por lo que quien observe irregularidades a este respecto deberá informar a la dirección.
4. Cada empleado debe ser informado individualmente de estas políticas. Adicionalmente las mismas deben ser publicadas en los medios internos de divulgación.

RESPONSABILIDADES

1. Alta Dirección

- La política de seguridad y ciberseguridad de la información son definidas, aprobadas por la dirección, publicadas, comunicadas y conocidas por las partes interesadas.

- Establecer, implementar, mantener y mejorar continuamente el sistema de gestión y seguridad de la información.
- Establecer y respaldar la política de ciberseguridad.
- Exigir a todo el personal que aplique la seguridad de la información de acuerdo a los procedimientos específicos de cada tema.
- Asignar recursos adecuados para implementar medidas de seguridad.
- Participar activamente en la gestión de incidentes de ciberseguridad.

2. **Área de Tecnología de la información (TI).**
   - Implementar y mantener medidas de seguridad técnicas.
   - Monitorear regularmente sistemas y redes para detectar amenazas.
   - Mantener actualizados los sistemas y aplicaciones con parches de seguridad.
   - Aceptar la responsabilidad personal de proteger los recursos de Tecnologías de Información y los activos de información de SETRACOL LTDA., contra la pérdida, modificaciones no autorizadas y accesos de terceras personas
   - Brindar un adecuado tratamiento a la información, que por sus funciones tenga a cargo, para garantizar que el registro, actualización y administración de la misma se haga de forma veraz, completa, exacta, comprobable y comprensible, haciendo uso de las herramientas tecnológicas dispuestas para ello y dando cumplimiento a las normas y mecanismos adecuados que garanticen su confidencialidad, integridad y disponibilidad.
   - Verificar y reportar, de forma periódica y oportuna, la existencia de novedades de información y adoptar las medidas necesarias para que los datos se mantengan protegidos.
   - Conservar con la debida seguridad la información recibida para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento.
3. **Empleados**
   - Aceptar y cumplir con las políticas y procedimientos de ciberseguridad implementados por la compañía.
   - Informar cualquier incidente o amenaza sospechosa al equipo de TI.
   - Proteger contraseñas y credenciales de acceso.
   - Guardar reserva sobre la información que les sea suministrada y utilizarla únicamente para los fines para los que le fue entregada.
   - Garantizar la reserva de la información, inclusive después de finalizada su relación contractual con SETRACOL LTDA.
   - Toda acción que intencionadamente retarde ponga en peligro o acceda a la información de otros usuarios, sin autorización específica, está prohibida, es éticamente reprobable y será sancionada con las normas administrativas y jurídicas, estipuladas por SETRACOL LTDA., y las autoridades competentes, si fuera necesario.

- Actuar de acuerdo con las Políticas de Seguridad de la Información y participar en las revisiones de seguridad que se lleven a cabo

4. Terceras partes

Los contratos o acuerdos de tercerización total o parcial para la administración y control de los activos de información y/o de los recursos de TI, como por ejemplo servicios de auditoría externa, de ajustes en la infraestructura de TI, entre otros, deberán contemplar los siguientes aspectos:

- Cumplimiento de la Política de Seguridad de la Información de SETRACOL LTDA.
- Comunicaciones que garanticen que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, estén informados y comprometidos con sus responsabilidades en materia de seguridad de la información.
- Definiciones relacionadas con la protección de datos.
- Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos de SETRACOL LTDA.
- Procedimientos a través de los cuales en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.

MEDIDAS DE SEGURIDAD

1. Todas las plataformas deben cumplir con los siguientes requerimientos de seguridad:

a. Mecanismos obligatorios que permitirán a los usuarios y administradores, compartir recursos e información y evitar la propagación de derechos de acceso inapropiados.
b. El sistema debe estar en capacidad de identificar a cada individuo, además de permitir asociar al usuario con acciones auditables.
c. El sistema debe estar en capacidad de proteger de modificaciones, accesos no autorizados o destrucción que puedan atentar contra los recursos del sistema.

La empresa podrá monitorear el uso de las herramientas de su propiedad, dadas a los empleados para el desempeño de sus funciones, tales como equipos de cómputo, software de oficina, correos, Internet, teléfonos, celulares, etc.

2. Restricciones de acceso:

a. Ningún empleado debe tener acceso a todas las opciones de una aplicación, a excepción del administrador del software.

b. Las transacciones contables relacionadas con las operaciones que las generan deben ser de uso exclusivo del área contable.

c. En cualquier caso, a través de los sistemas de información existen mecanismos que permiten identificar quién realizó una transacción, cuándo y desde qué terminal.

3. Uso de programas y aplicativos

- Se prohíbe instalar programas no autorizados por el área de Tecnología.

- Se prohíbe copiar programas o aplicativos de uso corporativo o alterar el software instalado. El licenciamiento es propiedad de SETRACOL LTDA y no puede ser transferido de alguna forma a un computador que no sea parte de la organización.
- Ningún usuario podrá usar programas que no estén autorizados por el área de tecnología o por las directrices de la compañía.
- Para el correcto desempeño de las labores cotidianas en cuanto a programas y aplicativos se refiere, los usuarios deberán dirigirse o comunicarse directamente con el área de sistemas, para el mantenimiento, solución de incidencias, fallas o problemas presentados sobre alguno de los aplicativos. Queda expresamente prohibido que un usuario trate de hacer mantenimiento o reparación sobre algún aplicativo del equipo.

4. Uso y manejo de la Información

La información es uno de los activos más importantes de la organización por lo tanto debemos cumplir con las siguientes normas y directrices para el correcto manejo de la misma:

- El uso del correo electrónico y del servicio de internet está permitido únicamente para fines corporativos o de desarrollo de las actividades necesarias para el funcionamiento de la organización. Lo anterior es verificado por el área de tecnología.

- Está prohibido divulgar información reservada de la empresa a otros funcionarios o terceros sin la debida autorización.

- Se prohíbe guardar información reservada de la empresa en dispositivos extraíbles como USB, CD´s, u otros medios sin la debida autorización.

- La organización se reserva el derecho a filtrar el contenido al que los usuarios puedan ingresar a internet, así como está prohibido el uso de Facebook, Instagram en general de redes sociales y redes P2P, así como bajar programas, contenido de adultos y pornografía entre otros. SETRACOL LTDA., posee el derecho para monitorear y registrar los accesos realizados desde los equipos de la organización. Cuando se requiera acceder a alguno de los contenidos filtrados, podrá solicitarlo al área de tecnología mediante el jefe inmediato, describiendo por qué se necesita dicho acceso.

- No podrá usarse el internet o los recursos tecnológicos de la empresa para usos ilícitos, o que atenten contra la ética, la misión y los valores de la empresa.

- Carpetas compartidas: cuando se tenga acceso a un recurso compartido o de la red, los usuarios que posean privilegios de cambio de la información son los directos responsables de lo que suceda con la misma, puesto que

de acuerdo a la política de backups, estos se sacan a ciertos horarios, por tanto, el uso indebido de la información quedará con respaldo al día anterior y la responsabilidad es directamente del usuario que modifica dicha información.

5. Correo Electrónico

Todos los mensajes del correo electrónico llevan la imagen corporativa, es por eso que está prohibido el uso del correo para las siguientes actividades:

- Enviar información a una o más de una persona de la empresa que no haya sido solicitada o no sea de su competencia.
- Enviar información, imágenes o videos al interior o exterior de la empresa, de pornografía, violencia, matoneo, acoso, burlas y otras actividades denigrando la moral y las buenas costumbres.
- Fomentar el uso de cadenas de correo ya que generan brechas de seguridad y atentan directamente sobre la productividad de los individuos de la organización.
- Usar el correo electrónico para hacer promociones y propuestas comerciales.
- Divulgar información de instituciones políticas, militares, religiosas ya que esta herramienta es exclusiva para uso corporativo.

NOTA: el uso del correo electrónico nos evita mantener información escrita acumulada, de así que tratemos de imprimir solo los correos que sean estrictamente necesarios, para apoyar el cuidado del medio ambiente y también los gastos de consumibles de la impresora.

6. Recomendaciones generales:

1. Se recomienda configurar los parámetros de seguridad del navegador de Internet para filtrar archivos que puedan dañar a la computadora, así como los parámetros de contenido para restringir el acceso a sitios de alto riesgo.
2. Cualquier archivo que se reciba por Internet deberá revisarse para asegurar que no contenga virus, ya que existen algunos que pueden destruir toda la información del disco duro del equipo. Antes de abrir cualquier archivo recibido por Internet, el usuario debe asegurarse de que sea un archivo confiable.
3. Se prohíbe la instalación de programas y la modificación de los programas, paquetes y configuraciones ya instaladas en los equipos.
4. No deje prendido la pantalla de su computador, sin hacer uso de ella por largos periodos de tiempo, si va a dejar de usarlo permanentemente, cierre las aplicaciones (navegadores o clientes de correo) que esté usando y siempre bloquee la pantalla al levantarse de su puesto.
5. Cambie con frecuencia sus claves de acceso a servicios y no se las comunique a nadie, (de preferencia, que sus contraseñas incluyan letras, mayúsculas y minúsculas, números y caracteres especiales, que sean de una longitud mínima de 8 caracteres.

6. No instale software libre (freeware o shareware) a menos que esté seguro que su uso no alterará el correcto funcionamiento de su computadora.
7. No desactive el monitor de antivirus de su equipo.

7. Antivirus

Nuestros sistemas deben contar con un sistema de antivirus que permita salvaguardar la información de la empresa frente al acceso no autorizado de personas y debemos hacer su respectiva actualización cuando el encargado lo informe.

Proceso recomendado a usuarios para prevenir problemas de virus

- Todo computador de la empresa debe tener instalado y en operación el antivirus conforme a las necesidades de la empresa.
- No abrir archivos o macros adjuntas a un correo de procedencia desconocida, sospechosa o fuente no confiable. Borré los archivos adjuntos y luego vacié su papelera de reciclaje.
- Borre el spam, cadenas y cualquier correo basura. No realice reenvío de los mismos.
- Nunca descargue archivos de sitios desconocidos o fuentes sospechosas.
- Evite compartir directamente los discos del ordenador con permisos de lectura / escritura.
- Siempre revise con el antivirus sus unidades de disco flexible, discos removibles o memorias flash ante de usarlas.
- Respalde información crítica y configuración de sistemas en forma regular y almacene la información en un lugar seguro.

POLÍTICA DE BACKUP DE LA INFORMACIÓN

Se realizará copia de los archivos considerados importantes de cada computador, la cual será realizada por el proveedor de TI. Para ello, se destinan diferentes equipos y programas. Se garantiza copias locales y copias en la nube para la información sensible.

POLÍTICA Y ACCIONES PARA CONSTRUIR CONTRASEÑAS SEGURAS

1. Se deben utilizar al menos 8 caracteres para crear la clave y en lo posible que contenga letras, números y signos.

2. Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.

3. Las contraseñas hay que cambiarlas con una cierta regularidad, recomendamos hacerlo mínimo cada 90 días.

POLITICA PARA EL USO DE INTERNET

Acceso a sitios de internet

1. Los usuarios utilizarán únicamente los servicios para los cuales están autorizados. No deberán usar la cuenta de otra persona, ni intentar apoderarse

de claves de acceso de otros, así como no deberá intentar acceder ni modificar archivos que no son de su propiedad, y mucho menos, los pertenecientes a la empresa.

2. Se debe respetar la privacidad de otros usuarios. Los archivos, discos, cintas e información son privados; el Usuario no debe intentar leer, copiar o cambiar los archivos de otro usuario, a menos que haya sido autorizado por éste.
3. Si no está navegando por el Web, cierre todas las ventanas abiertas de su explorador.

I. SANCIONES

El incumplimiento de esta política puede resultar en acciones disciplinarias, incluyendo la terminación del empleo o acciones legales.

Esta política de ciberseguridad debe ser comunicada a todos los empleados y revisada de forma regular para garantizar su eficacia en la protección de los activos digitales de la organización. Además, es esencial adaptar esta política a las necesidades específicas y a la evolución de las amenazas cibernéticas.

_____

Luis Eduardo Herrera Ruiz
Gerente general Setracol

Agosto 2023

SOCIALIZACIÓN

NOMBRE	CARGO	FECHA SOCIALIZACIÓN	FIRMA
