SERACIS
Seguridad más allá de la simple Vigilancia

POLÍTICAS DE SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN GQ62

30/04/2020
Versión 03

Contenido

1. INTRODUCCION

Una Política de Seguridad de la información es un modelo eficaz de normas para la organización que son entregadas a los empleados para su estricto cumplimiento. A su vez; es un documento único en el que se plasman las distintas caracterizaciones de los escenarios disponibles y las buenas prácticas de uso, así como los riesgos y vulnerabilidades que puedan afectar la información disponible en cualquier medio existente. Los objetivos de una política de seguridad de la información son la preservación de la confidencialidad, integridad, disponibilidad y el no repudio de la información. La Confidencialidad implica la protección de los activos contra accesos no autorizados, la Integridad garantiza que no exista perdida de datos que alteren la información, la Disponibilidad se refiere al acceso continuo a los activos de información y el no repudio gestiona la responsabilidad auditable del uso del recurso asignado. Esta política mejora continuamente para adaptarse de acuerdo con la evolución de la organización y los requisitos de TI (tecnologías de la información).

La política de seguridad de la información de la empresa desempeñará un papel importante para la toma de decisiones, pero no deberá modificar su estrategia y/o misión. Por lo tanto, se acopla al marco estructural y cultural existente para apoyar la continuidad, la productividad y la innovación garantizando así un ambiente seguro para la compañía, y no como una política de genéricos que impida a la organización y a sus integrantes el cumplimiento de su misión y sus objetivos.

Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware, los datos y documentos impresos. Estas medidas deben estar acorde a la pertinencia, importancia, vigencia y la naturaleza de riesgos previsibles de la información. Es compromiso de todos tener un lugar de trabajo bajo un ambiente seguro, en el que la confidencialidad, la integridad y la disponibilidad esté garantizada a nivel de red y de almacenamiento de información en todos los medios que se manejen; ya sean físicos o digitales.

Esta política es de estricto cumplimiento por cada uno de los empleados y hace parte de sus responsabilidades, compromiso y hábitos de trabajo. Con lo anterior; se pretende el uso adecuado de los distintos activos de información y recursos de la empresa. Su incumplimiento será objeto de las medidas y sanciones que ameriten.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Crear una política de seguridad de la información que vele por los pilares fundamentales: confidencialidad, integridad, disponibilidad y no repudio.

2.2 OBJETIVO ESPECÍFICO

• Desarrollar una guía para toda la compañía para el uso adecuado de activos físicos y lógicos de información.
• Minimizar el riesgo de los procesos misionales de la entidad.
• Cumplir con los principios de seguridad de la información.
• Cumplir con los principios de la función administrativa.
• Mantener la confianza de los funcionarios, contratistas y terceros.
• Apoyar la innovación tecnológica.
• Implementar el sistema de gestión de seguridad de la información.
• Proteger los activos de información.
• Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
• Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del SERACIS LTDA
• Garantizar la continuidad del negocio frente a incidentes. Alcance/Aplicabilidad
• Aplicar a toda la entidad, sus funcionarios, contratistas y terceros de SERACIS LTDA.

3. POLÍTICAS

3.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

SERACIS LTDA. ha venido adelantando un plan de sistematización el cual incluye aplicativos de uso específico, instalados en servidores que permiten accederlos desde estaciones de trabajo. Estos puestos están dotados con computadores personales en los que se han instalado las aplicaciones y herramientas, debidamente licenciadas, que la empresa cree necesarias para el correcto desempeño de sus funciones. Los puestos de trabajo cuentan con acceso a redes tanto internas (área local) como externas (internet) para el envío de correos a clientes y compañeros de trabajo, para compartir información requerida por otras áreas de la empresa y para consultas a sitios web que permitan mantener actualizada la información manejada.

La información es quizás el activo más valioso de una compañía por lo que su confidencialidad y seguridad son una responsabilidad de todos los empleados. Con el propósito de asegurar la información de SERACIS se deben seguir estrictamente las siguientes reglas:

1. No divulgar información confidencial de la empresa a personas no autorizadas o a empresas que lo soliciten con fines comerciales.
2. Los contratistas que intervengan equipos computo, bases de datos o archivos digitales deben firmar un acuerdo expreso de confidencialidad autorizado por la gerencia.
3. No debe almacenarse información valiosa de la compañía en los discos duros de los equipos; ya que no se hacen respaldos o backups de los mismos. Todo usuario cuenta con 1 TB en la nube asociado a su buzón de correo 4. El escritorio (desktop) de su equipo Windows no debe emplearse para almacenar datos de ninguna naturaleza.
5. Diariamente se realizan backups automáticos a las bases de datos y a los archivos compartidos según los mecanismos establecidos en el PT09 Respaldos y contingencia.
6. Seracis LTDA proveerá los mecanismos para que la información sea accedida y utilizada por el personal que de acuerdo con sus funciones así lo requiera. Sin embargo, se reserva el derecho de revocar al personal, el privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameriten.
7. Si la empresa procesa y mantiene información de usuarios externos que sean datos personales y/o sensibles de acuerdo con la normativa vigente, la organización se compromete a asegurar que esta información no será divulgada sin previa autorización y estará protegida de igual manera que la información interna.
8. Con el fin de velar por el correcto uso de los activos de información de su propiedad, Seracis Ltda. se reserva el derecho de auditar en todo momento y sin previo aviso, el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los activos de información.

Revisión de los derechos de acceso de los Usuarios

Los derechos de acceso de los usuarios a la información y a la Plataforma Tecnológica y de procesamiento de información de Seracis LTDA, debe ser revisada periódicamente y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo.

Retiro de los derechos de acceso

Cada uno de los procesos de la empresa es responsable de comunicar al área de gestión humana, el cambio de cargo, funciones o actividades o la terminación contractual de los colaboradores pertenecientes al proceso. El área de gestión humana es la encargada de comunicar al proceso de tecnologías de la Información sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

3.2 POLITICA DE SEGURIDAD INFORMÁTICA

Los equipos de cómputo asignados a los empleados son propiedad de SERACIS LTDA. y están disponibles para su trabajo única y exclusivamente. Tanto las licencias del software instalado como los datos almacenados son propiedad de SERACIS LTDA. y no deben ser usados para fines diferentes a los que la empresa designe. Para garantizar este objetivo se establecen las siguientes reglas:

1. El modelo de seguridad de SERACIS LTDA. es por capas de acuerdo con el modelo OSI.
2. Todos los equipos deberán tener instaladas las últimas actualizaciones de Windows, parches de seguridad y antivirus instalado.
3. Los equipos deberán estar conectados a un regulador de corriente o fuentes de energía continua; como medida de prevención de variaciones de electricidad.
4. Si se presentara una suspensión de servicio eléctrico; se debe dar prioridad de funcionamiento a los servidores. Por lo tanto, se deben apagar los equipos cuando se interrumpa el fluido eléctrico para ahorrar tiempo de carga.
5. Una vez al año se realizará una revisión de las redes en capa 1 (físico) y 2 (red).
6. Periódicamente, por espacio de 12 meses, se realizará una limpieza física a toda la infraestructura de equipo de cómputo por parte del personal de sistemas.
7. Toda actividad elaborada por el equipo de sistemas deberá de estar debidamente documentada para darle seguimiento y que sirva como evidencia en los procesos de auditoría interna.
8. No permitir o facilitar el uso de los sistemas informáticos de la empresa a personas no autorizadas.
9. No se permite el acceso a la red interna de la empresa a personas que no sean funcionarios de esta. Con la salvedad de funcionarios externos que provengan de entes de control, auditoria, funcionarios del grupo empresarial, entre otros, con autorización de la Gerencia.
10. No utilizar los recursos informáticos (Hardware, Software y datos) y de telecomunicaciones para otras actividades que no estén directamente relacionadas con las funciones del empleado dentro de la empresa. 11. Todos los equipos asignados tendrán deshabilitados los accesos a puertos USB, CD o Diskettes. Esta medida tiene 3 objetivos:

• Evitar ataques de virus en los equipos y el servidor.
• Evitar extracciones no autorizadas.
• Evitar la carga de archivos ajenos a la labor de gestión.

12. A todos los equipos se les realizará una revisión de virus por lo menos cada mes, que incluye las siguientes actividades.

- Actualizar su base de firmas de virus (actualización de la lista de amenazas)
- Búsqueda de virus (análisis del equipo)
- Eliminación de virus si fue detectado.

13. En caso de ser autorizado un usuario para el uso de memorias USB y discos extraíbles, es responsabilidad del usuario hacer uso del antivirus para que los equipos no sean infectados y proteger la información de la empresa en caso de pérdida. Los usuarios pueden pedir apoyo al área de TI para el uso de antivirus y cifrar la información almacenada.
14. El personal administrativo y administrativo a nivel operativo; tendrá una cuenta de correo electrónico, que les permite exclusivamente recibir y enviar información indispensable para sus actividades de trabajo si así lo requieren. Debe ser solicitada al área de TI mediante un ticket en mesa de ayuda puesto por su jefe inmediato y aplicar las medidas de protección descritas anteriormente.
15. El área de sistemas medirá la efectividad de la seguridad informática implantada analizando los eventos generales presentados en forma mensual haciendo énfasis en los incidentes; donde un mes sin incidentes es bueno, con un incidente es aceptable y mayor a uno es crítico. En todos los casos se deberán justificar los incidentes y gestionar el tratamiento para mitigarlos, controlarlos o transferirlos de acuerdo con el nivel del riesgo.
16. Las áreas de concentración de cableado, racks y servidores deben estar acondicionadas con UPS, aire acondicionado y cableado debidamente organizado a fin de garantizar la seguridad de la capa física.
17. Las áreas de concentración de cableado de las sedes principales deben estar protegidas con puerta con llave y alarma. Deben tener controlado el acceso de personal o proveedores. Además; debe solicitarse la autorización al personal de operaciones encargado para ingresar y se llevará un control documentado de accesos por el área de sistemas a fin de evitar alteraciones o desconexiones que generen incidentes.

3.3 POLÍTICA DE USUARIOS FINALES

Los equipos de cómputo de SERACIS LTDA. deben estar disponibles para el uso de los empleados de la empresa; donde cada equipo tiene un responsable quien deberá velar por su cuidado físico y lógico: por lo que debe seguir las siguientes reglas:
1. Es responsabilidad de los usuarios seguir estrictamente los lineamientos y protocolos de bioseguridad establecidos por la compañía.
2. Es responsabilidad de los usuarios mantener su lugar de trabajo aseado, ordenado y en condiciones que permitan acceder cómodamente y proteger a los equipos de cómputo y comunicaciones asignados.
3. Se debe limpiar el exceso de polvo exterior con un paño seco sin usar líquidos los elementos periféricos del sistema de cómputo como: teclado, mouse, pantalla y torre.
4. Como medida de higiene y seguridad del equipo físico informático (Hardware), queda totalmente prohibido sin excepción alguna el fumar, ingerir bebidas o alimentos mientras se estén utilizando las estaciones de trabajo, impresoras o cualquier otro equipo que tenga que ver con la

infraestructura informática, ya que este tipo de práctica pone en riesgo el buen funcionamiento de los dispositivos.
5. Como medida de protección, queda prohibido dejar objetos sobre los equipos de cómputo ya que esto puede ocasionar accidentes o sobrecalentamiento de los equipos, ocasionando cortos internos, daños del procesador, daño en los discos duros, de la memoria RAM y bajas en el rendimiento de estos, evidenciando un deterioro progresivo en los equipos.
6. Los computadores de la empresa solo deben usarse en un ambiente seguro. Por lo que está prohibido conectarse a redes Wifi distintas a las de la empresa o consultar sitios NO SEGUROS O SIN AUTORIZACIÓN empleando celulares o usando programas para evadir controles para acceder-los.
7. Los equipos de SERACIS LTDA. solo deben usarse para actividades de trabajo y no para otros fines.
8. Los equipos de cómputo deben tener pantalla limpia sin elementos en la ubicación escritorio del sistema operativo. 9. Todos los archivos que viajen por correo y que contengan información sensible deberán estar comprimidos con contraseña de uso interno como medida de seguridad de información.
10. Está terminantemente prohibido modificar la configuración de Software y Hardware establecida por el Departamento de Sistemas de SERACIS LTDA.
11. Los equipos no pueden moverse o reubicarse sin permiso. Para llevar un equipo fuera de la empresa se requiere solicitar la respectiva autorización a la Gerencia y/o a la Junta Directiva de SERACIS LTDA.
12. La pérdida o robo de cualquier componente del hardware, o programa de software, deberá ser reportada inmediatamente al área de TI o a la Gerencia de SERACIS LTDA.
13. No está permitido llevar al sitio de trabajo computadores portátiles personales y en caso de ser necesario, se requiere solicitar la respectiva autorización. 14. Los usuarios deberán abstenerse de divulgar o compartir sus datos de acceso a los programas y sesiones de Windows.
15. Los usuarios no deben copiar a un medio removibles (CD, USB, etc.) el software o los datos residentes en los computadores de SERACIS LTDA., para ser trasladados fuera de las instalaciones, sin la aprobación previa de la Gerencia.
16. No debe utilizarse Software descargado de internet y en general Software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el área de TI
17. Para prevenir acciones legales o virus informáticos, se prohíbe la instalación de Software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo no se permite el Software de distribución gratuita, a menos que haya sido aprobado previamente por área de TI.

18. Será responsabilidad del encargado del equipo de trabajo velar por el buen funcionamiento y cuidado del computador, por lo tanto, si se llegase a quebrantar esta política, recaerán sobre este las acciones pertinentes.
19. Reportar inmediatamente a su jefe inmediato y a los responsables del área de TI cualquier evento que pueda comprometer la seguridad de la información y sus recursos informáticos, como por ejemplo virus, modificación o pérdida de datos, correos fraudulentos y otras actividades inusuales.

3.4 POLÍTICA DE SEGURIDAD PARA LAS COMUNICACIONES

La red interna, la telefonía móvil o fija y el uso del internet solo deben emplearse para satisfacer las necesidades del trabajo que realice cada empleado de SERACIS LTDA. Las siguientes reglas definen la política de SERACIS LTDA. con respecto al uso de internet o de redes externas:
1. Toda la información escrita, descargada o enviada vía internet empleando los equipos de cómputo de la empresa es propiedad de SERACIS LTDA. Esto significa que la empresa podrá exigirle al responsable de cada equipo, la revisión de los datos almacenados en su equipo y monitorear la actividad en la red.
2. Todo empleado deberá asegurarse de que la información enviada por medio de correos electrónicos sea precisa, apropiada, ética, respetuosa y legal.
3. Solo podrán enviar correos con destinatarios diferentes a empleados SERACIS las personas autorizadas por el director del departamento correspondiente.
4. Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.
5. La navegación en Internet para fines personales no debe hacerse a costo en tiempo y recursos de SERACIS LTDA. De requerirse un uso diferente se debe contar con la autorización de la Gerencia y en el horario que se determine.
6. Está terminantemente prohíbo mostrar, descargar o enviar imágenes, mensajes o similares con contenidos sexuales, políticos, religiosos o étnicos.
7. Con el fin de velar por el correcto uso de las comunicaciones, Seracis Ltda. se reserva el derecho de auditar en todo momento y sin previo aviso, el uso correcto de los recursos en relación con el acceso y uso que los usuarios hacen; cualquier uso indebido será reportado al jefe inmediato.

3.5 POLÍTICA DE CONTROL DE ACCESO Y CONTRASEÑAS

El ingreso a las instalaciones o lugares que posean activos de información deben ser controlados, así como el mecanismo de protección que proveen los aplicativos para garantizar la seguridad de los datos es el de la autenticación. Cada usuario es dotado con Usuario o UserID y una Contraseña o Password que garantizan que la persona que está accediendo el equipo o el aplicativo es la correcta y por ende se le asignan los permisos para realizar sus labores específicas que serán monitoreados con el principio de no repudio para la verificación de responsables ante cualquier evento de modificación de datos. Las siguientes reglas deben ser seguidas rigurosamente:

1. Los visitantes de deben ser registrados y acompañados en todo momento a fin de evitar ingresos no autorizados a recursos tecnológicos.
2. Los centros de datos deben ser restringidos con control de acceso de doble factor y registro de ingreso por parte de personal técnico interno o externo si es el caso.
3. Su(s) contraseña(s) son personales e intransferibles. No divulgue ni preste su usuario y contraseñas a otros.
4. El usuario no debe guardar su(s) contraseña(s) en forma legible en los archivos de disco y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada.
5. Cuando el empleado abandone su estación de trabajo deberá bloquear el equipo de tal manera que el procedimiento de autenticación sea solicitado nuevamente al reiniciar la actividad.
6. El usuario debe cambiar su clave una vez sea notificado al inicio de sesión o cuando sea pertinente. Debe tener una complejidad mínima de 8 caracteres con combinación de mayúsculas, minúsculas, caracteres especiales y números independientemente de que el sistema lo exija. No se permiten claves que contenga el nombre de la empresa o el nombre del usuario por considerarse débiles y vulnerables. 7. Todos los accesos a los programas principales estarán protegidos mediante un mecanismo de usuario y contraseña, así como permisos de acceso. De igual forma, las sesiones de Windows personales estarán protegidas con contraseña de acuerdo con el numeral 4.
8. Si no cuenta con un usuario y clave para acceder a su equipo o requiere un permiso específico para algún activo de información; deberá solicitarlo a través de la mesa de ayuda por medio de su jefe directo.

3.5 POLÍTICA DE SOPORTE TÉCNICO

1. Todo equipo de cómputo de la empresa será relacionado en el formato de calidad FT03 ACTA DE ENTREGA DE EQUIPOS DE CÓMPUTO V2 y deberá ser firmado por el usuario responsable de uso.

2. Los mantenimientos periódicos del equipo serán respaldados en el formato FT02 Formato de Mantenimiento de equipos
3. Cada empleado tiene asignado un equipo de cómputo al cual debe ingresar con un usuario y contraseña. En caso de no tenerla debe solicitarla el jefe directo al área de TI a través de la mesa de ayuda de TI.
4. El personal debe hacer uso adecuado de los recursos informáticos (PC, impresoras, programas, correo, etc.) y el personal de sistemas debe asegurar que se cumpla esta política.
5. Para solicitar permisos específicos a recursos de red programas o información de la red; debe solicitarlo el jefe directo a la mesa de ayuda de TI.
6. Todo el personal deberá informar a sistemas sobre requerimientos generales, cualquier novedad, falla de programas, daño físico, mal uso del equipo de cómputo y la afectación de activos de información a través de la mesa de ayuda dispuesta en la dirección de correo mesadeayuda@seracis.com para su adecuado seguimiento y posterior solución.

Fecha de revisión: 30 de abril de 2020

ELABORA	REVISA	APRUEBA
SERGIO ANDRÉS ÁLVAREZ	SARA HENAO CADAVID	LUIS FERNANDO CARVAJAL
Coordinador de sistemas	Directora de Proyectos y Calidad	Representante Legal