POLÍTICA ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

701001 | Julio 2024 | Versión 005

- **Política de dispositivos móviles**
  - Se deben adoptar medidas de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles.
  - Todo dispositivo móvil (iPad, teléfonos inteligentes, laptops, entre otros) con acceso a la red de COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3, bien sean de propiedad de COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3 o personal, deberán sin excepción, ser configurados con los controles mínimos definidos en el procedimiento de uso de dispositivos móviles.
  - El computador portátil (laptop) que contenga información confidencial deberá contar con el cifrado de su disco duro.
  - Está prohibido el uso de funciones de equipos móviles como medio de almacenamiento, grabación y capturar información de la empresa al que el usuario no esté autorizado por COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3.
  - En caso de pérdida o hurto de un dispositivo móvil que se encuentre autorizado para acceder a las aplicaciones o información de COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3, se debe notificar de manera inmediata al área respectiva TI con el fin de tomar las medidas respectivas y evitar accesos no autorizados a la información.
- **Política de Trabajo remoto (Teletrabajo):**
  - El/los directores(es) o líder(es) de área debe(n) asegurar los mecanismos necesarios para la aseguración de la información que esté respaldada en los equipos o servidores en cuestión.

- Se deben realizar periódicamente auditorías y/o revisiones de vulnerabilidades a los servidores y/o equipos de cómputo que hacen parte de la conexión remota final para la reducción de amenazas.
- El trabajo remoto sólo se debe dar mediante autorización o notificación del personal de TI de la empresa.
- Toda conexión remota sea de empleados o de proveedores de COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3, puede ser monitoreada y podrá ser bloqueada en caso de identificar situaciones inusuales respecto al uso de los activos de información.
- Esta modalidad podrá establecerse a Colaboradores que puedan desempeñar sus funciones desde casa.
- Es obligación de todo el personal estar disponible durante el horario laboral establecido y a requerimiento de su jefe, en los medios de comunicación acordados (Teléfono personal, teléfono fijo, correo electrónico, Skype, conexión de internet y de canales seguros etc.).
- Es responsabilidad del jefe inmediato planear y supervisar las actividades del personal en “Teletrabajo o Home Office” y del envío de los entregables del Colaborador para analizar el cumplimiento y productividad.

Política de control de acceso

- Deben existir procedimientos y estándares formales establecidos para la creación, modificación y eliminación de usuarios, roles y perfiles.
- La cuenta de usuario o identificador debe ser única para cada empleado y contratista.
- Se debe acceder a los sistemas de información o dispositivos de red a través de la cuenta de usuario asignada, la cual debe cumplir con los controles y estándares de seguridad definidos.
- La contraseña es personal e intransferible y no puede ser compartida por ningún motivo, la misma debe cumplir con los estándares y controles de seguridad definidos.
- La definición de roles y perfiles está basada en el menor privilegio requerido para el correcto desempeño de sus funciones.
- Deben existir controles que permitan monitorear las diferentes acciones realizadas por los usuarios garantizando la trazabilidad y registro de evidencias.
- Las cuentas genéricas deben tener asignada la responsabilidad de su utilización a un usuario y deben ser utilizadas exclusivamente para

establecer comunicación con otro recurso informático o de red, dichas cuentas no deben ser de uso personal.

- Las cuentas privilegiadas deben ser utilizadas, exclusivamente para el mantenimiento y atención de incidentes sobre los recursos informáticos o de red, las mismas deben ser custodiadas y monitoreadas por el dueño del activo.

- **Política sobre el uso de controles criptográficos y protección y vida útil de las claves criptográficas durante toda su vida útil.**

  - Se debe asegurar el uso adecuado y eficaz de cifrado para proteger la confidencialidad, la autenticidad y/o la integridad de la Información.

  - Se deben desarrollar e implementar controles criptográficos para la protección de la información.

  - Para la gestión de claves se deben desarrollar e implementar controles para el uso, protección y gestión del ciclo de vida de las claves de cifrado, a lo largo de su ciclo de vida.

  - A continuación, se definen a los cargos encargados del manejo de los distintos tipos de controles y llaves criptográficas de la compañía:

    - Manejo de certificados SSL: Desarrollador Master
    - Manejo de las Suites de Cifrados de los servidores: Desarrollador Master
    - Manejo del cifrado Bitloker: director TIC
    - Manejo de los tokens financieros: Gerencia

- **Política de escritorio y pantalla limpios**
  - Se debe adoptar controles para mantener el escritorio limpio aplicado a documentos físicos y digitales, así como mecanismos de pantalla limpia para las instalaciones de procesamiento de información.

  - En el escritorio físico no se debe dejar información de tipo confidencial a la vista de personal no autorizado, si se encuentra este tipo de información u otra de tipo secreta se puede generar un incidente de seguridad de la Información.

- Al ausentarse temporalmente del equipo, cada usuario deberá bloquear su sesión para que personal no autorizado, no pueda sustraer, validar y eliminar información sensible.

Política de respaldo

- La información sensible que se encuentra almacenada en las plataformas tecnológicas de COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3 y de proveedores, debe contar con acciones de restauración que garanticen la integridad de la información en casos de emergencia y según sea requerido y autorizado por el responsable del activo de la información.

- De acuerdo a la criticidad de la información se deben definir políticas de copias diarias, semanales, mensuales, anuales de tipo incremental y total; igualmente se debe definir restauraciones periódicas de archivos aleatorios manteniendo un registro como evidencia.

Políticas y procedimientos de transferencia de información

- Se debe proteger la información transferida de la intercepción, la copia, la modificación, el ruteo incorrecto y la destrucción.

- Proteger la información electrónica sensible comunicada en forma de elemento adjunto.

- Se prohíbe expresamente la transferencia de información que incluya la difamación, el acoso, el reenvío de cartas de cadena y las compras no autorizadas, como también divulgar información confidencial por cualquier medio.

- Se debe concienciar al personal que no deberían sostener conversaciones confidenciales en lugares públicos o a través de canales de comunicación, oficinas abiertas y lugares de encuentro inseguros.

- **Política de seguridad en el desarrollo seguro, adquisición y mantenimiento de sistemas de información**

  - Asegurar que la segregación de funciones sea mantenida tanto a nivel de usuario como en ambientes controlados y claramente diferenciados (desarrollo, pruebas, producción).

  - Establecer controles que permitan dar cumplimiento a los requerimientos de seguridad establecidos en los procesos de desarrollo y soporte.

  - Establecer metodologías y procedimientos de desarrollo y adquisición de software que integren requerimientos de seguridad en el desarrollo de código, manejo de fuentes, programas y objetos.

  - Se deben identificar los activos de información y los riesgos asociados para nuevos desarrollos o proyectos, con el fin de establecer los controles para el aseguramiento de la información.

  - Las transacciones deben estar protegidas para prevenir la transmisión incompleta, errores de enrutamiento y alteraciones no autorizadas de los mensajes o su reenvío.

  - Debe protegerse la información involucrada en los cambios a los sistemas en el ciclo de vida de desarrollo y a las plataformas de producción y aplicaciones críticas, mediante procesos formales de control de cambios.

  - Los datos de salida de los aplicativos que manejan información sensible deben contener los datos relevantes requeridos para el uso de acuerdo al rol y se deberán enviar exclusivamente a los usuarios y/o terminales autorizadas.

  - Los aplicativos de la empresa deben pasar por un proceso de pruebas y aceptación en un ambiente dedicado para tal fin antes de ser liberados a producción.

  - El acceso a la información contenida en las bases de datos sólo está permitido a través de las aplicaciones de los sistemas de la empresa. Sólo tendrán acceso los usuarios autorizados que de acuerdo a su rol se identifican mediante usuario y contraseña. En casos excepcionales el

propietario de la información debe autorizar a la compañía de hacer uso de estas facultades.

- Los sistemas de procesamiento y almacenamiento de información de los sistemas operativos y aplicaciones, deben contar con los últimos parches de seguridad provistos por el fabricante debidamente aprobado e instalado, con el fin de dar el aseguramiento adecuado.

- Con el fin de preservar la confidencialidad de la información, a efectos de no vulnerar las condiciones de seguridad de acuerdo con su clasificación, la información que está en producción no debe ser utilizada para desarrollo de pruebas. En casos excepcionales el propietario de la información debe autorizar a la compañía de hacer uso autorizado de los datos personales.

- Para todo desarrollo se debe considerar la seguridad de la información desde el inicio del proceso de diseño de los sistemas, pasando por cada una de las fases de desarrollo hasta su liberación a producción.

- **Política de seguridad de la información para las relaciones con el proveedor**
  - Todos los contratos o acuerdos definidos deben contar con acuerdos de confidencialidad de la información.

  - Las partes interesadas deben conocer, aceptar y dar cumplimento a las políticas, procedimientos y estándares de seguridad de la información establecidos por la organización.

  - Se debe acordar y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos.

  - Los Proveedores, contratistas o terceros vinculados a la empresa deben garantizar que el intercambio de información desde y hacia COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3 cumple con las exigencias que éste defina con base en las leyes y regulaciones vigentes, así como también las políticas de seguridad de la información en dicho documento, por tanto, dichas disposiciones deben quedar integradas en los contratos que se suscriban.

Política de contraseñas

- Todos los empleados de COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3 recibirán un identificador de usuario y una contraseña de acceso a cada recurso informático.
- El empleado es responsable de la administración y buen uso de sus identificadores de usuario y contraseñas, garantizando en todo momento su confidencialidad.
- Siendo el empleado, la primera línea de defensa ante intrusiones y accesos no autorizados, este deberá generar contraseñas que se consideren de difícil reconocimiento, sea a través de técnicas de ingeniería social o mediante herramientas tecnológicas de descubrimiento de claves.
- Se considera una contraseña segura aquella cuya longitud es mayor a ocho (8) caracteres, contiene letras, número y al menos un (1) carácter especial. Todos los empleados de COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3 deberán ceñirse a esta consideración a la hora de generar sus contraseñas.
- Las contraseñas deberán ser cambiadas, al menos, cada tres (3) meses.

Política de salida de equipos para el trabajo en casa

COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3 cuenta con los mecanismos para que los empleados realicen sus labores desde casa, previa autorización del líder área. Para tal fin, deberán conectarse a través de la VPN instalada en el equipo portátil asignado para su labor.
Los equipos considerados para usar durante el trabajo en casa deben cumplir con las siguientes especificaciones:

- Tener el directorio activo configurado
- Discos internos encriptados
- Antivirus actualizado
- VPN instalada y funcionando

En caso de que el equipo no cuenta con todo lo anteriormente mencionado, no podrán ser retirados de las oficinas de COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3, dicha confirmación

debe ser entregada por el área TI. El área TI es la encarga de instalar el software de VPN para la conexión y dar las indicaciones al funcionario para lograr una conectividad exitosa y cuente con el acceso a sus recursos.

- **Política de instalación de software en sistemas operativos**

La política de instalación de software en sistemas operativos es fundamental para garantizar la seguridad y la eficacia de los sistemas informáticos de una organización.

- Todo software para instalar en los sistemas operativos deberá ser aprobado por el área de TI de COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3.
- El software debe ser instalado por personal autorizado por el área de TI.
- Antes de la instalación de cualquier software, se debe realizar un análisis para determinar si el software es compatible con los sistemas operativos existentes.
- La instalación de software debe realizarse con los permisos necesarios y los privilegios de administrador correspondientes.
- Los usuarios no deben instalar ningún software en los sistemas operativos sin la autorización previa del área de TI.
- Todo software debe ser adquirido legalmente y tener una licencia valida.
- El software debe ser actualizado regularmente para garantizar la seguridad y la estabilidad de los sistemas operativos.
- Todo software debe contar con un soporte técnico para garantizar su funcionamiento de manera eficiente con una solución disponible y en un tiempo aceptable, de tal manera que no afecte la operación de COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3.
- Se debe proporcionar capacitación adecuada a los usuarios y al personal técnico en los aspectos de operación y funcionalidad de los nuevos sistemas de información o mejoras a sistemas de información existentes, antes de su puesta en marcha.

Restricciones sobre la instalación de software

- Solo se permite la instalación de software aprobado, los usuarios no deben instalar software en los equipos asignados. Cualquier instalación por realizar lo deben solicitar al área de TI. Esto significa que solo se permite la instalación de software que ha sido aprobado por el personal de TI de COMERCIALIZADORA DE SOFTWARE SERVICIOS Y

SUMINISTROS S.A.S - CS3 y solicitado por un director de área, además se debe verificar que este se encuentre debidamente licenciado.

En COMERCIALIZADORA DE SOFTWARE SERVICIOS Y SUMINISTROS S.A.S - CS3, las solicitudes de instalación de software deben hacerse a través de un ticket de soporte en el SAC. Después de recibir la solicitud, el área de TI investiga el software solicitado, verifica licenciamiento, evalúa la seguridad y la fuente del programa, y determina si se puede o no instalar en el equipo de la empresa.

Expresa total conocimiento y en función del cargo se propone a mantenerlas el gerente de Comercializadora de software, Servicios y Suministros S.A.S – Sigla CS3.S.A.S

Luis Adolfo Contreras V.

LUIS ADOLFO CONTRERAS VILLEGAS
Representante Legal