CONTENIDO

1. OBJETIVO

Este documento tiene como finalidad comunicar a los colaboradores, Socios de Negocios, Proveedores y Clientes, las Políticas de Seguridad de la Información establecidas por la Presidencia de la Entidad, las cuales buscan la protección adecuada de la información con respecto a la integridad, disponibilidad y confidencialidad de la misma sin importar el medio por el cual sea distribuida o almacenada, manteniendo la Política de Seguridad de la Clínica actualizada a efectos de asegurar su vigencia y nivel de eficacia.

Con lo anterior, Proteger los recursos de información de la Clínica y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

1.2 OBJETIVOS ESPECÍFICOS:

- Minimizar el riesgo en los procesos de la clínica.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de protección de datos personales alineándose al
- cumplimiento de la ley 1581 de 2012.
- Mantener la confianza de los funcionarios, contratistas, proveedores, aliados
- estratégicos y otros terceros.
- Apoyar la innovación tecnológica en la clínica.
- 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 y contratistas.
- Garantizar la continuidad del negocio frente a incidentes.

2. ALCANCE

Esta política general y todas las políticas específicas y procedimientos que se deriven del Sistema de Gestión de Seguridad de la Información son de obligatorio cumplimiento para:

- Todos los funcionarios de CLINALTEC, incluyendo empleados con contratos a término fijo, término indefinido, temporales, estudiantes en práctica, estudiantes del SENA, y otras figuras de contratación que se adopten.

- Todos los funcionarios de terceras partes como Clientes, socios de Negocios, Proveedores, Compañías de Outsourcing, auditores externos, consultores externos y en general cualquier tipo de usuario de los sistemas de Información de la organización.

3. TERMINOLOGÍA

- **ACTIVOS DE INFORMACIÓN:** Recursos del sistema de información o relacionados con éste, necesarios para que la Entidad funcione correctamente y alcance los objetivos propuestos por su dirección.

- **CIFRADO:** Es el proceso que se aplica a unos datos para hacerlos incomprensibles. Este proceso o transformación precisa de una clave de cifrado, que es una cadena aleatoria de bits, de una

medida determinada (como, se denomina, de una determinada longitud de clave). Sólo aplicando el proceso contrario, denominado descifrado, a los datos cifrados será posible regenerar los datos originales y, por tanto, hacerlas otra vez comprensibles.

- **CLASIFICACIÓN DE LA INFORMACIÓN**: Es la decisión para asignar un nivel de sensibilidad a los datos cuando se están creando, corrigiendo, almacenando o transmitiendo. Un esquema de clasificación debe usarse para definir un conjunto apropiado de niveles de protección y comunicar las medidas especiales de tratamiento.

- **CONTROLES:** Medidas para garantizar que los riesgos sean reducidos a un nivel aceptable.

- **DUEÑO DE LA INFORMACIÓN:** Es responsable de la información que le sea asignada, así como de la clasificación, control y monitoreo del uso y gestión de la misma. Son Dueños de Información todas aquellas personas de CLINALTEC que tienen bajo su responsabilidad parte o la totalidad de la información. Los responsables de la información son encargados de preservar los principios de seguridad de la información (integridad, disponibilidad y confidencialidad) y deben coordinar la implementación de políticas con otros dueños de información y con custodios de la información. Los dueños deben especificar cómo se debe utilizar la información y cómo se debe proteger, además de definir cómo se administrarán los procedimientos de seguridad de la información y cómo se aplicarán los niveles apropiados de protección para cada una de las clases de información (pública, privada y confidencial).

- **IMPACTO:** Daño producido a la Entidad por un posible incidente o evento, y resultado de la agresión sobre un activo, visto como diferencia en las estimaciones de los estados de seguridad y operación, obtenidas antes y después del evento.

- **INCIDENTE**: Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos, inesperados o no deseados, de seguridad de la información que tienen una probabilidad significativa de poner en peligro las operaciones y procesos del negocio y amenazar la seguridad de la información. Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos, sistemas de información, procesos del negocio o recursos tecnológicos de CLINALTEC.

- **INFORMACIÓN:** Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

- **INFRAESTRUCTURA TECNOLÓGICA:** Todos los componentes tecnológicos que están al servicio de la entidad.

- **INFRAESTRUCTURA:** La tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones.

- **ISO 27001:** Código de práctica para la administración de la seguridad de la información de la Organización Internacional para la Estandarización (ISO).

- **MONITOREO:** Es aquella actividad que pretende hacer seguimiento periódico y revisión de ciertas tareas realizadas en los sistemas de información.

- **NORMA:** Guía general de Seguridad de la Información sobre un tema específico, pero independiente de la plataforma tecnológica. La norma está sustentada en una política y regula parte o la totalidad del objetivo de la misma.

- **OFICIAL DE SEGURIDAD DE LA INFORMACIÓN**: Es el responsable de implementar la estrategia de seguridad de la información alineada con los objetivos del negocio, dirigir el programa de seguridad de la información y tomar las decisiones que permitan gestionar la seguridad de la información en el marco de control y cumplimiento definido y aprobado por la Entidad.

- **PROCESO**: Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.

- **RIESGO:** Es la probabilidad de que una amenaza se concrete sobre uno o más activos causando daños o perjuicios a la Organización por medio de una vulnerabilidad o punto débil.

- **ROL/PERFIL:** Conjunto de funciones, normas, comportamientos y derechos definidos en un sistema de información que se espera que un usuario cumpla o ejerza de acuerdo a su nivel adquirido o atribuido en CLINALTEC.

- **SEGURIDAD DE LA INFORMACIÓN:** Es la preservación de la confidencialidad, integridad y disponibilidad de la información; otras características también pueden estar involucradas, tales como la autenticidad, responsabilidad, aceptabilidad y confiabilidad.

- **SISTEMA DE INFORMACIÓN:** Conjunto de programas o aplicaciones desarrollados en diferentes lenguajes de programación, que facilitan el manejo de la información generada por los diferentes procesos de la Entidad.

- **TI**: Tecnología de información.

- **PRACTICANTE**: Personal que desempeña labores en la empresa bajo contrato de aprendizaje SENA, pasante o practicante universitario y estudiantes de colegio realizando su servicio social obligatorio.

- **TEMPORAL:** Personal contratado por una cooperativa de trabajo asociado trabajando en misión en CLINALTEC.

4 CONDICIONES GENERALES

4.1 RESPONSABILIDADES

De acuerdo al punto 5.3 de la **NTC-IEC-ISO 27001 versión 2013,** Los siguientes entes son responsables, en distintos grados, de la seguridad en la Clínica:

- **El Comité de Seguridad de la Información**: Definir, documentar y verificar el cumplimiento de las políticas, normas, estándares y guías de seguridad de la información alineadas con los objetivos institucionales.

- **El Oficial de Seguridad de la Información:** Evaluar, diseñar y coordinar la implantación de los controles administrativos, técnicos y operativos que garanticen un alto nivel de seguridad de la Información que permitan a la organización el normal y eficiente desarrollo de los procesos con información confiable, íntegra, veraz, oportuna y con eficiencia operativa.

- **Dueño de la información**: rol asignado a los funcionarios encargados de clasificar la información con el fin de proteger su integridad, confidencialidad y disponibilidad. Estos funcionarios deben proteger la información, sin embargo, las labores de administrar dicha información recaen en el rol llamado custodio de la información.

- **Custodio de la información**: rol asignado a los funcionarios que tienen la responsabilidad de llevar a cabo las actividades de seguridad designadas por el dueño de la información, como probar las copias de respaldo, validar la integridad de la información, sugerir mejoras de seguridad para la información y administrar la información según su clasificación.

- **Los usuarios:** rol asignado a los funcionarios que tienen acceso a la información y hacen uso de ella para realizar sus funciones. Tienen la responsabilidad de hacer cumplir los controles de seguridad definidos por los dueños de la información.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE CLINALTEC

Los activos de información y los equipos informáticos son recursos importantes y vitales de la Clínica. Sin ellos se podría quedar rápidamente fuera del negocio y por tal razón la Presidencia y la Junta Directiva o quien haga sus veces, tienen el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, Crackers, interrupción de servicio, accidentes y desastres naturales, garantizar la no obsolescencia de la Tecnología (software, hardware y redes).

Los distintos jefes de proceso, están en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos. En todo caso, cada año el Comité Seguridad de la Información llevará a cabo un análisis de riesgos y se revisarán las políticas de seguridad. Así mismo, se preparará al final de cada año un informe para la Presidencia y la Junta Directiva, que muestre el estado actual de la Compañía en cuanto a Seguridad de la información.

A todos los empleados, consultores y contratistas debe proporcionarles capacitación, información, y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos de la Compañía. Debe hacerse hincapié en que la seguridad de la información es una actividad tan vital para la Compañía como lo son la contabilidad y la nómina.

5.1 POLÍTICAS ESPECÍFICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

- El Sistema de Gestión de Seguridad de la Información de CLINALTEC se implementa dentro del marco de la norma NTC ISO/IEC 27001 en su última versión.

- El presente documento, así como todas las políticas y procedimientos de seguridad de la información que se deriven del SGSI deben ser comunicadas a todos los funcionarios de la Organización.

5.1.1 REVISIÓN DE LA POLÍTICA DE SEGURIDAD

1) Oficial de seguridad de la Información es responsable por la actualización permanente del documento de Política de Seguridad de la Información de CLINALTEC, en sus principios rectores, políticas específicas, procedimientos, estándares y guías de uso.

La actualización debe ser realizada (mandatoriamente) en la medida en que ocurra alguno (o varios) de los siguientes eventos:

- Cambios en el ambiente de negocios o estrategia empresarial (ejemplo: nuevas estrategias de mercado, nuevos productos, cambios de prioridades, fusiones o cesiones, cambios en la estructura organizacional, proyectos específicos y nuevas gerencias, etc.)
- Cambios en la infraestructura de riesgos de seguridad de información de la compañía. Estos cambios pueden ser como consecuencia de un análisis de riesgos y vulnerabilidades o por aparición de nuevas vulnerabilidades y/o amenazas que cambien el perfil de riesgo de la infraestructura técnica de la Organización.
- Nuevas obligaciones legales y/o reglamentarias o cambio de las existentes que afecten el procesamiento de la información, intercambio de información con terceros, etc.
- Avances en las mejores prácticas de seguridad de la Información registradas en el código de prácticas ISO/IEC 27002 o cambios en la norma ISO/IEC 27001, o las que apliquen en su momento y que previamente evaluadas sean necesarias para la organización.
- Aplicación de nuevos controles identificados como resultado de los análisis de los incidentes de seguridad de la información o el resultado de auditorías de TIC.

2) Es responsabilidad del Oficial de Seguridad de la Información informar a la Compañía y terceros la actualización y publicación de nuevas versiones de este documento.

5.1.2 ORGANIZACIÓN DE SEGURIDAD

1) La Presidencia de CLINALTEC, se encargará de dar una dirección estratégica al sistema de Gestión de Seguridad de la Información acorde con los lineamientos de la Organización y aprobará los principios rectores, políticas específicas y procedimientos que hacen parte de este documento, pero delega las responsabilidades operativas de la Seguridad de la Información al Comité de Seguridad de la Información, el cual estará conformado por los siguientes integrantes:

  - Oficial de Seguridad de la Información
  - Presidente o su representante.
  - Gerente de proyectos TIC.
  - Coordinador de Recursos Humanos.
  - Delegado de la Oficina Jurídica.

- Otras áreas invitadas a tratar temas específicos.

2) La Presidencia revisará periódicamente las actas e informes del Comité de Seguridad de la Información

3) El Comité de Seguridad de la Información coordinará las actividades relacionadas con la Administración y operación del Sistema de Gestión de Seguridad de la Información.

4) Otras responsabilidades del Comité de Seguridad de la Información son:

- Revisar y aprobar la Política de Seguridad de la Información de CLINALTEC, los principios rectores, políticas específicas, procedimientos, estándares y guías de uso de los temas relacionados a seguridad informática.
- Evaluar, revisar, aprobar e implementar los controles de seguridad de la información basados en la gestión del riesgo.
- Identificar las tendencias y los cambios importantes de los riesgos de seguridad informática de la Organización y proponer los cambios de políticas y procedimientos adecuados con el fin de controlar las vulnerabilidades identificadas.
- Asegurar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios.
- Establecer mecanismos de control que permitan medir el cumplimiento de las Políticas y Procedimientos de Seguridad de la Información.
- Recomendar acciones correctivas a los incidentes de seguridad reportados.
- Hacer seguimiento a los incidentes de seguridad reportados.
- Establecer mecanismos de control de la información confidencial de la Clínica
- Gestionar las sanciones aplicables por incumplimiento a las Políticas de Seguridad de la Información, principios rectores, políticas específicas, procedimientos, estándares y guías de uso de los temas relacionados a seguridad informática.
- Coordinar revisiones periódicas al Sistema de Gestión de Seguridad de Información, realizadas por consultores externos o internos, cuando el nivel de experiencia y capacitación lo permita.
- Realizar reportes periódicos a la Presidencia de Empresa indicando el nivel de seguridad obtenido mediante la ejecución de los controles del Sistema de Gestión de Seguridad de Información.
- Desarrollar programas de concientización y capacitación a todos los funcionarios que enfaticen la importancia del cumplimiento del Sistema de Gestión de Seguridad de la información y su contribución al logro de los objetivos del negocio.
- El comité de seguridad de la Información realizará sus reuniones en el evento en que ocurra uno (o varios) de los siguientes eventos:

  - Hayan pasado máximo 6 meses después del último comité de seguridad informática.
  - Ocurrencia de un incidente de seguridad que requiera una sesión especial del comité (ver política de administración de incidentes de seguridad).
  - Ocurrencia de un evento por el cual sea necesaria la declaración de contingencia técnica y/u operativa.

5.2 DISPOSITIVOS MÓVILES Y TELETRABAJO [ISO/IEC 27002:2015 A.6.2]

5.2.1 COMPUTACIÓN MÓVIL Y TRABAJO REMOTO:

- **COMPUTACIÓN MÓVIL: [ISO/IEC 27002:2015 A.6.2.1]**

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarque la protección física necesaria, el acceso seguro a los dispositivos, la utilización de los dispositivos en lugares públicos, el acceso a los sistemas de información y servicios de la Clínica a través de dichos dispositivos, las técnicas criptográficas a utilizar para la transmisión de información clasificada, los mecanismos de resguardo de la información contenida en los dispositivos y la protección contra software malicioso.

- **TRABAJO REMOTO**: **[ISO/IEC 27002:2015 A.6.2.2]**

El trabajo remoto sólo será autorizado por el Director o Gerente de área, a la cual pertenezca el usuario solicitante, conjuntamente con el Responsable de Seguridad Informática, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

Como quiera que la CLÍNICA INTERNACIONAL DE ALTA TECNOLOGÍA - CLINALTEC tiene las aplicaciones CORE de su negocio locales y algunas otras en ambientes web como son Correo electrónico y repositorios de datos de usuarios entre otros; es muy importante para la seguridad de la labor de los colaboradores de la clínica que se tengan en cuenta medidas mínimas de seguridad de la información, para así cumplir con el objetivo de mantener disponibilidad, confidencialidad e integridad de la información de la clínica.

En los casos que se requiera que un funcionario esté en modo trabajo remoto es importante que éste trabaje con el equipo local y activo de la clínica y solo en casos especiales sea aprobado trabajar con equipos que no son de la clínica siendo un requisito que estos cumplan con las medidas de seguridad mínimas que esta política contempla. Para que un funcionario esté en modo trabajo remoto es un requisito que se tengan las mínimas medidas de seguridad para estar protegido frente a las principales amenazas de Internet, estas son:

- Disponer de un antivirus licenciado y actualizado.
- Utilizar un equipo con sistema operativo legal licenciado y actualizado
- Utilizar contraseñas robustas en todos sus accesos requeridos basados en la política de contraseñas de la clínica.
- Verificar que en el acceso a los servidores corporativos se utilicen certificados reconocidos por la red de la clínica, un usuario del dominio de la clínica y que los sitios web a los que acceda tengan el “candado” de la conexión SSL.

Para prácticamente cualquier otro tipo de conexión que requiera acceso a la red interna de la organización, lo más importante es activar una conexión VPN, con un usuario y clave válida dentro de la red de la clínica, así como contar con los permisos respectivos de su jefe o director de área.

Para casos especiales cuando el colaborador no puede usar un equipo de la clínica, éste permiso deberá ser avalado por un directivo de la misma y este colaborador deberá firmar un documento de responsabilidad para el cumplimiento de la política en cuanto a que el equipo a usar no debe ni puede tener menos de las medidas de seguridad descritas en esta política y que la responsabilidad de los eventos de seguridad que pasen en la infraestructura por el incumplimiento de la misma será su responsabilidad.

5.3 SEGURIDAD DEL PERSONAL [ISO/IEC 27002:2015 A.7]

5.3.1 CUMPLIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

- Es obligación de los usuarios, sin excepción alguna, conocer, respetar, cumplir y hacer cumplir las políticas de seguridad de la información de CLINALTEC.

- La responsabilidad de seguridad es parte de los términos y condiciones del empleo. La violación o no cumplimiento de cualquiera de las directrices documentadas en las políticas de seguridad de la información establecidas por CLINALTEC, serán argumentos para la aplicación de acciones disciplinarias, incluyendo la terminación del contrato.

5.3.2 ACUERDOS DE CONFIDENCIALIDAD

- Todos los empleados, sin importar el tipo de contrato, ya sea a término fijo o indefinido, deben firmar un acuerdo de confidencialidad en el momento en que ingresan a CLINALTEC.

- Todo el personal vinculado con la Clínica como contratista, trabajador en misión, contrato de aprendizaje, practicante, etc., también debe firmar un acuerdo de confidencialidad en el momento del inicio de sus labores en CLINALTEC.

5.3.3 PROCESOS DISCIPLINARIOS

1) Todo el personal que cometa un fallo de seguridad, por ejemplo, la violación deliberada de estas políticas de seguridad de la información, debe ser sancionado mediante un proceso disciplinario ejecutado por el área de Talento Humano para el caso de funcionarios de CLINALTEC o a través de contratos o procesos jurídicos en caso de terceros.

2) Los procesos disciplinarios pueden incluir una serie de acciones en función de la gravedad de la violación, iniciando por memorandos con copia a la hoja de vida del infractor hasta la cancelación del contrato laboral y acciones legales para recuperar las perdidas y los daños consecuentes.

3) Para el caso de funcionarios de CLINALTEC, los procesos disciplinarios a los que se someterán los empleados que no cumplan las políticas de seguridad son:

   - Llamado de atención por parte del comité de seguridad de la Información, en donde se detalle el incumplimiento y las causas que puede generar.
   - En caso de reincidencia, se enviará un llamado de atención con copia a la Hoja de vida y al jefe inmediato.
   - En caso de reincidencia, el empleado se suspenderá de sus actividades por un lapso de 3 a 5 días dependiente de la gravedad del incidente.
   - En caso de reincidencia continua, se cancelará su contrato laboral.

4) Si el incidente afecta económicamente o la reputación de CLINALTEC, se realizarán las acciones civiles correspondientes de acuerdo a la legislación colombiana.

5.3.4 CONOCIMIENTO, EDUCACIÓN Y ENTRENAMIENTO DE SEGURIDAD DE LA INFORMACIÓN

- Talento Humano es responsable del desarrollo de planes de capacitación, educación y sensibilización en seguridad de la información y uso adecuado de los recursos tecnológicos para todos los funcionarios.

- Todo el personal debe participar en las sesiones de concientización frente a temas de seguridad de la información. Un resumen impreso de las medidas de seguridad básicas de la información se debe proporcionar a cada empleado, temporal, contratista o practicante y guardar una copia firmada en archivo.

- Talento Humano con asesoría del Oficial de Seguridad de la Información, deben desarrollar estrategias de sensibilización, entrenamiento y educación en seguridad de la información, para promover conocimiento constante a todos los empleados, temporales, contratistas y practicantes. La estrategia de sensibilización de seguridad debe consistir en entrenamiento y resúmenes impresos constantes.

5.3.5 TERMINACIÓN O CAMBIO DE EMPLEO DE LOS FUNCIONARIOS

- El personal que se retira de CLINALTEC debe recibir por parte del Jefe de Área un recordatorio acerca de los compromisos legales y éticos adquiridos con respecto a mantener la confidencialidad de la información a la cual tuvo acceso en el curso de su empleo.

- Consideraciones similares deben ser aplicadas cuando un funcionario de CLINALTEC cambie de funciones en una misma área o en áreas diferentes. En este caso, los jefes involucrados en la transferencia del personal, deben tramitar que el acceso a la información confidencial de las áreas involucradas es protegido de accesos o modificaciones no autorizadas.

- Todo el personal, sin importar el tipo de vinculación laboral, que se retire de CLINALTEC, debe entregar al jefe de área y/o Jefe de TI los activos informáticos asignados para su cargo (incluyendo documentos, archivos digitalizados, computadores, información de Clientes almacenada en teléfonos móviles o computadores de mano, dispositivos de almacenamiento USB, etc.).

- Cada Jefe de Área debe informar las novedades (ingresos, retiros, reemplazos, traslados, etc.) de las personas a su cargo al Jefe de TI solicitando la asignación, modificación o desactivación de los permisos y perfiles de cada usuario, según sea el caso.

- El acceso a la información, computadores, redes de datos e instalaciones físicas, deben ser revocadas de inmediato cuando un funcionario o un tercero se retira de CLINALTEC.

5.3.6 INVESTIGACIÓN DE EMPLEADOS

- Talento Humano debe realizar una investigación a todo candidato potencial que pueda llegar a ser empleado de la Entidad. Esto puede incluir pruebas psicológicas, referencias personales y laborales, verificación de la educación, entre otros. Si el empleado se está buscando a través de terceros o una agencia apropiada, debe seguirse como mínimo los mismos análisis definidos para la investigación los cuales deben ser llevados a cabo por la agencia.

- Los empleados contratados para cargos en los cuales deban tener acceso a información confidencial de la Entidad debe tener investigación adicional de acuerdo con las necesidades definidas en las leyes o regulaciones.

5.4 GESTIÓN Y ADMINISTRACIÓN DE ACTIVOS DE INFORMACIÓN
5.4.1 RESPONSABILIDAD DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios o responsables de los activos de información deben ser claramente designados por la Presidencia de CLINALTEC o los jefes respectivos de cada área. Los propietarios serán los responsables de la protección de los activos de información contra incidentes de seguridad.

- Los propietarios de los activos de información, son responsables por la clasificación de sus activos y la definición y auditoría constante de las restricciones de acceso y otros controles de seguridad de la información

5.4.2 INVENTARIO DE LOS ACTIVOS DE INFORMACIÓN

1) Los responsables de los activos de información deben realizar un inventario de los datos (información) almacenados en las estaciones de trabajo y bases de datos de los servidores, así como de los documentos en medio físico necesarios para el desarrollo de las actividades.

2) Los datos mínimos que debe contener el inventario de los datos (físicos y magnéticos) son:

   - Nombre del archivo o documento
   - Ubicación (carpeta física o lógica)
   - Responsable
   - Custodio
   - Clasificación de la información de acuerdo a los criterios de esta política.
   - Existencia de alguna copia.
   - Identificar quien o quienes tienen acceso a la información

3) El inventario de los datos y documentos físicos (activos de información) debe ser actualizado en la medida en que ocurra uno o varios de los siguientes casos:
   - Cambios en el ambiente de negocios o estrategia empresarial.
   - Nuevas obligaciones legales o reglamentarias.
   - Pasado un año después de la última actualización del inventario.

4) El Jefe de TI debe realizar el inventario de los aplicativos y programas bajo licencia con que cuenta la organización. Los datos que debe incluir el inventario son:
   - Nombre del aplicativo o software
   - Versión
   - Número de licencias adquiridas por la Organización
   - Número de licencias instaladas

5) El Jefe de TI debe realizar el inventario de los activos de información tangibles (computadores, impresoras, equipos de comunicaciones, etc.). Los datos mínimos que debe contener el inventario de activos son:

- Nombre del equipo
- Marca
- Modelo
- No. De serie
- No. De activo
- Ubicación
- Usuario a cargo

6) El inventario de los activos de información tangibles debe ser actualizado en la medida en que ocurra uno o varios de los siguientes casos:
   - Cambios en el ambiente de negocios o estrategia empresarial
   - Renovación o actualización tecnológica.
   - Desarrollo o compra de un sistema de información (aplicativo)
   - Pasado un año de la última actualización del inventario.
   - Depreciación y amortización de activos (software, hardware licencias, etc.).

5.4.3 CLASIFICACIÓN DE LA INFORMACIÓN

1) Los responsables de la información en medio físico y magnético deben realizar la clasificación de acuerdo a los criterios de confidencialidad, sensibilidad, riesgo de pérdida o compromiso, aspectos legales, requerimientos de retención y facilidad de recuperación que deben ser empleados.

2) Los requerimientos legales, estatutarios y regulatorios deben ser considerados al momento de evaluar la clasificación de la información.

3) La clasificación de la información debe ser realizada simultáneamente con el inventario.

4) Los criterios para clasificar la información son:

a. Información de uso público o informativo:

- Su divulgación no requiere de autorización especial dentro y fuera de la compañía y su función es de comunicación del personal en general.
- Puede darse a conocer al público en general a través de carteleras, Intranet, memorandos, etc. No se requiere brindar las garantías para que no existan problemas de disponibilidad o de denegación en su consulta.
- Su modificación debe ser realizada exclusivamente por los autores y el personal asignado para esas tareas.

b. Información de uso interno o privada

- Su divulgación no autorizada, principalmente fuera de la organización sería inadecuada o inconveniente, debe ser de conocimiento únicamente por parte de los funcionarios de la organización.

- Puede ser compartida entre áreas dada su necesidad para la operación diaria y no consolida resultados finales de gestión.

c. Información de uso confidencial

- Sustenta estrategias del negocio, información financiera consolidada, informes de gestión para junta y gerenciales, registros para toma de decisiones, información de Clientes y competencia, información de personal y cualquier otra que pueda comprometer la seguridad de la empresa o de las personas.

- Su divulgación no está autorizada, incluso dentro de la organización, por el impacto de daño que puede causar a la Compañía. Debe ser usada únicamente por ciertos funcionarios de la Compañía quienes son responsables de su manejo.

5) La Organización determina que la información de los Clientes es clasificada como confidencial, por lo tanto, su manejo debe ser exclusivo para personas debidamente autorizadas y está limitado a actividades propias del Negocio, está totalmente prohibida su divulgación a personas no autorizadas.

6) La información no puede desclasificarse o disminuir su nivel de clasificación sin llevar a cabo un análisis de los riesgos que esto implica, y una aprobación por el responsable de la información. Este determinará si su información puede moverse a una clasificación más baja o más alta basado en las definiciones de clasificación desarrolladas por CLINALTEC.

5.4.4 ROTULACIÓN Y TRATAMIENTO DE LA INFORMACIÓN

1) La información impresa debe ser rotulada en cada página con la clasificación de la información definida para dicho documento. Los documentos electrónicos deben tener la etiqueta de clasificación en el encabezado o en el pie de cada página.

2) Todos los documentos que contienen información altamente sensible deben tener una portada o etiqueta donde se identifique su clasificación.

5.4.5 CONTROLES PARA LA INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL

1) El envío a un tercero (incluyendo los Clientes/Pacientes) de información clasificada como confidencial debe ser autorizado por el responsable de la información.

2) La información clasificada como confidencial que sea necesario enviar a un tercero (incluyendo los Clientes), debe ser transmitida utilizando mecanismos de criptografía.

3) La información confidencial en medio físico debe ser almacenada en áreas con acceso físico controlado, de tal forma que se garantice que solamente el personal autorizado tiene acceso a ella.

4) Se debe llevar un log que permita realizar una trazabilidad de los cambios realizados a la información confidencial almacenada en medios magnéticos. El log debe identificar el responsable, fecha y hora del cambio.

5) Cualquier información electrónica eliminada de sistemas informáticos y documentos impresos deben ser destruidos de tal forma que se proteja la confidencialidad de la información.

5.5 CONTROL DE ACCESO

5.5.1 POLÍTICA DE CONTROL DE ACCESO LÓGICO

1) Todos los recursos informáticos y/o aplicativos de CLINALTEC deben usar controles de acceso lógico, con el fin de prevenir el acceso no autorizado a la información confidencial de la Organización.

2) El acceso lógico a los recursos informáticos de CLINALTEC debe ser controlado en función de los requerimientos de la Organización.

3) El control de acceso a la información debe ser definido, aprobado y documentado por los responsables de la información y deben estar basados en requerimientos específicos del negocio.

4) Se deben crear perfiles de acceso asociados a roles que tienen responsabilidades y cumplen con actividades comunes (cargos); estos perfiles deben permitir el acceso mínimo y suficiente para el adecuado desempeño de las actividades de los usuarios (política de menor privilegio). Los permisos de acceso a los aplicativos deben ser garantizados por cargos y no por funcionarios.

5) Los permisos de acceso a las redes, servicios y sistemas de información de CLINALTEC, serán otorgados mediante un proceso de aprobación que asegure el tener acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.

6) Todos los empleados y personal externo que acceden a los sistemas de información quedarán registrados y dispondrán de credenciales personales e intransferibles, con lo cual será responsable de mantener su confidencialidad y asegurar su correcto uso.

7) Se deben deshabilitar o actualizar los privilegios de acceso a los recursos informáticos inmediatamente se presente la novedad correspondiente o cuando se genere un cambio de privilegios en un rol o perfil.

8) Cuando un empleado o un usuario externo deja la Institución o cambia de posición, se deben eliminar o reasignar sus privilegios de acceso a los recursos informáticos de CLINALTEC

9) El responsable de la Información debe realizar una comparación periódica entre los requerimientos de acceso de los usuarios a los aplicativos y el nivel de acceso con que realmente cuentan y verificar que los usuarios que efectivamente acceden la información corresponden a los autorizados previamente por él.

10) Los aplicativos deben ser el único vehículo para acceder los datos de producción de CLINALTEC.

11) Está totalmente prohibido el uso de usuarios compartidos en los sistemas de información.

12) La Coordinación TIC debe garantizar que todos los usuarios que tienen acceso a cuentas privilegiadas tienen sus propias cuentas personales para el uso diario. El uso de estas cuentas debe ser rastreado y monitoreado periódicamente.

5.5.2 REGISTRO DE USUARIOS

1) A cada usuario interno y/o externo de la Organización que requiera acceso a los sistemas de información, se le asignará un único código de usuario, el cual es de carácter personal e intransferible.

2) Los usuarios de los recursos informáticos de CLINALTEC no deben compartir su código de usuario / contraseña o cualquier mecanismo otorgado para su identificación y autenticación. La responsabilidad que un usuario de CLINALTEC adquiere al recibir su código de usuario / contraseña o cualquier mecanismo de identificación y autenticación se extiende a todo tipo de interacción que ese identificador tenga con el sistema.

3) La creación, modificación y eliminación de cuentas de usuarios debe ser realizada mediante un procedimiento formal y debe ser autorizado por el responsable de los datos.

4) Debe existir un procedimiento formal para deshabilitar los códigos de usuario que no requieren el acceso a los sistemas de información por un periodo de tiempo determinado. Ejemplo funcionarios que salen de vacaciones, licencias, etc. Está totalmente prohibido que las áreas utilicen los códigos de usuarios de funcionarios que se encuentren ausentes de La Empresa. En caso de que se requiere el acceso a un aplicativo, es necesario hacer la solicitud formal para otro funcionario mediante el procedimiento establecido.

5) La eliminación de accesos y servicios de red asociados a un código de usuario debe ser realizada inmediatamente el usuario ha finalizado su vinculación laboral, contractual o comercial con CLINALTEC o ha cambiado de rol dentro de la Organización y no se requiere que acceda a estos recursos informáticos. Talento Humano es responsable por reportar a la Oficina TIC's las novedades presentadas con los funcionarios sin importar el tipo de vinculación laboral con la Clínica (temporales, de planta, practicantes SENA, etc.). Los jefes de las áreas son responsables por reportar a la Oficina TIC's las novedades de usuarios pertenecientes a consultores, asesores, auditores externos y otros terceros que tengan acceso a los sistemas de información.

6) La Coordinación TIC's debe conservar un registro de la solicitud, entrega y eliminación de los usuarios.

7) La Coordinación TIC's debe garantizar que los usuarios internos y externos firmen una declaración en la que certifican que reciben el usuario y la contraseña y se comprometen a cumplir las políticas de seguridad y garantizar su confidencialidad.

5.5.3 POLÍTICA DE ADMINISTRACIÓN DE CONTRASEÑAS

1) Las contraseñas deben cumplir con el siguiente estándar:
   - Longitud mínima de (12) caracteres
   - Alfanumérica
   - Debe contener mayúsculas y minúsculas.
   - Debe contener por lo menos 2 caracteres especiales.

2) La contraseña expira cada 60 días y debe ser cambiada por los usuarios. El sistema avisará 10 días antes que se debe cambiar la contraseña

3) No se permite repetir ninguna de las últimas 10 contraseñas

4) El sistema debe solicitar el cambio de la contraseña de manera obligatoria la primera vez que se ingrese al sistema.

5) Los sistemas de información deben permitir que los usuarios puedan crear y modificar sus propias contraseñas.

6) Los sistemas de información deben exigir que los usuarios confirmen su contraseña.

7) Los sistemas deben almacenar y transmitir las contraseñas de modo seguro.

8) La Coordinación TIC's debe asegurar que las computadoras, las bases de datos y aplicaciones que almacenan la cuenta de usuario y la contraseña, restringen el acceso sólo al personal autorizado. Este acceso debe ser revisado trimestralmente y debe coincidir con la revisión técnica del empleado, contratista, temporal, practicante; del servidor y el usuario utilizados.

9) Los usuarios internos y externos que presenten 3 intentos fallidos en el momento de digitar la contraseña, la cuenta debe ser bloqueada y no pueden tener acceso al sistema de información al cual está intentando acceder. Estas cuentas deben ser desbloqueadas manualmente por la Mesa de Servicio. La identidad de los usuarios que solicitan restablecer la contraseña debe ser verificada antes de restablecer la contraseña.

10) Los usuarios deben asegurar que las contraseñas no están escritas o almacenadas en los sistemas de información en archivos no protegidos. Los usuarios no deben copiar nombres de usuarios y/o contraseñas en los scripts o archivos de texto claro, trabajos por lotes o la documentación de procesos.

11) La Coordinación TIC's, debe garantizar que las cuentas de usuario que no hayan sido utilizadas por 90 días se deshabilitan automáticamente.

5.5.4 INICIO DE SESIÓN SEGURO

1) Antes de una conexión exitosa, CLINALTEC debe garantizar que la información de identificación de la Entidad, la red, la ubicación o el nombre del equipo no son divulgados.

2) La Coordinación TIC's debe garantizar que, en el momento de ingresar a los sistemas de información, se le informa al usuario que:
   - El sistema debe ser utilizado únicamente por usuarios autorizados
   - Mediante el uso del sistema, el usuario acepta que él o ella es un usuario autorizado
   - Es consciente que está siendo monitoreado al utilizar este sistema.

3) La Coordinación TIC's, debe garantizar que los sistemas operativos o sistemas de información que proveen servicios de autenticación no transmiten las contraseñas en texto claro.

4) La Coordinación TIC's, debe garantizar que los sistemas de información no ofrecen a los usuarios toda la información sin antes haber iniciado sesión. El proceso de acceso no debe ofrecer ninguna

'Ayuda' o revelar que característica de la secuencia de inicio de sesión (ID de usuario o contraseña) es incorrecta.

5.5.5 RESTRICCIONES EN EL PERÍODO DE USO DE LAS SESIONES

1) La Coordinación TIC's debe garantizar que las sesiones del sistema operativo que se encuentran inactivas durante 5 minutos, son automáticamente cerradas.

2) La Coordinación TIC's, debe asegurar que no se permita a los usuarios disponer de varias sesiones en el mismo sistema.

5.5.6 POLÍTICA DE USO DEL CORREO ELECTRÓNICO

1) El servicio de correo electrónico es para uso exclusivo de las actividades relacionadas con el trabajo de cada funcionario.

2) El envío de información clasificada como confidencial, debe ser aprobado por el Jefe de Área o el Dueño de la Información. Para el envío de esta información, es recomendable utilizar algún mecanismo de cifrado o protección mediante password.

3) Se prohíbe la difusión no solicitada de puntos de vista personales referentes a temas políticos, raciales y religiosos, al igual que la inclusión de mensajes sobre creencias, frases célebres, convocatorias políticas entre otros, al igual que usar el email para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular

4) Se prohíbe fomentar el envío de cadenas de mensajes, recepción o envío de mensajes con archivos adjuntos con extensiones .exe, .avi, .mp3, .vbs, .mpg, .jpg los cuales corresponden a archivos de video, música, gráficos, juegos, ejecutables, etc.

5) Este servicio no debe usarse para enviar SPAM o mensajes no solicitados ni tampoco para enviar material obsceno e ilegal o relacionado a pornografía infantil o cualquier clase de pornografía.

6) Está prohibido configurar reglas en los buzones de correo electrónico que reenvíen los mensajes a servidores públicos de Internet como Outlook, Gmail, etc.

7) No se puede utilizar el correo electrónico, para intimidar, insultar o acosar a otras personas, interferir con el trabajo de los demás provocando un ambiente de trabajo no deseable dentro del contexto de las políticas de La Empresa.

8) No se puede usar para la transmisión, distribución, almacenamiento de cualquier material protegido por las leyes vigentes. Esto incluye sin limitación alguna, todo material protegido por derechos de autor (copyright), Marcas registradas, secretos comerciales u otros de propiedad intelectual.

9) El tamaño de los archivos adjuntos no debe exceder el estándar definido por La Coordinación TIC's, este tamaño puede ser chequeado por medio de las propiedades de cada archivo. Si el archivo adjunto excede este tamaño, es necesario comprimir el archivo.

10) El nivel de almacenamiento de los buzones no puede exceder el estándar definido por la Coordinación TIC's, por lo tanto, el usuario debe eliminar periódicamente los mensajes leídos de modo tal que no exceda esa cuota. En caso de que el usuario requiera ampliación de esta capacidad, debe ser autorizada por el La Coordinación TIC's

11) La firma predeterminada solo puede contener nombre y apellidos, cargo, extensión y nombre de la compañía.

12) Está prohibido adjuntar firmas escaneadas.

13) En caso de recibir un mensaje bajo sospecha de virus, (de personas desconocidas con asuntos desconocidos o sospechosos) no se debe abrir y se debe reportar de inmediato a la Oficina TIC's y/u Oficial de Seguridad de la información.

14) No está permitido el uso de cuentas de correo personales o de servicios de correo externo como Outlook, Yahoo!, Gmail, etc., para transmitir o intercambiar información referente o perteneciente a CLINALTEC

5.5.7 POLÍTICAS DE USO DE INTERNET

1) El acceso a internet debe ser aprobado por el CSI de CLINALTEC.

2) El acceso a internet está restringido únicamente a páginas de información financiera, técnica, médica, comercial, cultural, etc., a las cuales por desarrollo de las actividades propias de cada cargo sea necesario ingresar para consultar información que faciliten las labores relacionadas al cargo.

3) El acceso a internet NO puede ser utilizado para los siguientes propósitos:

- Actividades relacionadas a juegos online por internet
- Ingreso a cualquier material considerado como pornográfico, ofensivo, discriminatorio o ilegal según las normas internas de La Empresa y la legislación
- Ingreso a páginas de pornografía infantil
- Ingreso a Redes sociales como Facebook, Twitter, LinkedIn, etc, a menos que sea autorizado por Presidencia, o se requiera por las funciones del usuario.
- Descargar música, videos, fotos, fondos de pantalla, programas, juegos etc. los cuales representan un alto riesgo de virus y daños al computador y de legalidad en su uso por derechos de autor.
- Utilizar los servicios de PELÍCULAS, RADIO y TV por demanda.
- Utilizar los servicios de Internet para enviar archivos que sean confidenciales y de propiedad exclusiva de CLINALTEC.
- Cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocios particulares.
- Utilizar los servicios de internet para la transmisión, distribución o almacenamiento de cualquier archivo protegido por las leyes vigentes. Esto incluye todos los archivos protegidos por derechos de autor, marcas registradas, secretos comerciales u otros de propiedad intelectual.

- El acceso no autorizado a cualquier intento de prueba, verificación o rastreo (scan) de vulnerabilidades de un sistema o red, violando las medidas de seguridad o de autenticación sin la expresa autorización del propietario del sistema o la red.
- No se podrán utilizar los servicios de internet corporativo para establecer comunicaciones vía chat sin el VoBo del líder correspondiente.

5.6 SEGURIDAD FÍSICA Y DEL ENTORNO

5.6.1 ÁREAS DE ACCESO RESTRINGIDO

1) Se define como aquellas áreas que necesitan autorización previa para permitir el ingreso de personas ajenas al área, por la naturaleza de la información confidencial que se maneja o los procesos que allí se realizan. Dentro de la Organización fueron identificadas las siguientes:

   - Oficina TIC's
   - Centro de Cómputo Torre Clínica
   - Centro de Cómputo Edificio TIC's
   - Gerencia Médica
   - Gerencia Financiera
   - Contabilidad
   - Facturación
   - Oficina Jurídica.
   - Archivo.
   - Almacén.

5.6.2 CONTROL DE ACCESO FÍSICO A LAS DEPENDENCIAS DE CLINALTEC

1) El ingreso de dispositivos de grabación de audio, fotos y video a las áreas de acceso restringido o áreas seguras está totalmente prohibido.
2) CLINALTEC debe asegurar que los derechos de acceso a todas las instalaciones son revisados anualmente. El acceso a lugares considerados áreas seguras, debe ser revisado regularmente.
3) Todos los visitantes, empleados, temporales, contratistas y practicantes deben ser autorizados para la entrada física a las instalaciones la CLINALTEC
4) Los funcionarios de la CLINALTEC deben portar en un lugar visible el carnet de identificación como funcionarios.
5) Los visitantes, temporales, contratistas y practicantes deben portar un carnet que los identifica como visitantes ocasionales. Este carnet debe ser de un color diferente al de los funcionarios de CLINALTEC
6) La autorización del acceso de visitantes a las áreas seguras está en cabeza de la Presidencia o el delegado de ésta de acuerdo al procedimiento establecido según corresponda.
7) Una vez autorizado el ingreso del visitante, el funcionario visitado deberá recogerlo y acompañarlo todo el tiempo durante el recorrido o su permanencia en el área segura.
8) Todos los visitantes a las áreas seguras deben firmar una lista de control de acceso antes de ingresar al área. En esta bitácora se debe registrar entre otros los siguientes datos: nombre del visitante, la fecha, la hora de entrada y de salida y la persona que es visitada. Esta bitácora debe estar disponible para efectos de auditoría por un periodo no inferior a un año.

5.6.3 PROTECCIÓN DE CENTROS DE CÓMPUTO

1) Los centros de cómputo de CLINALTEC, deben incorporar medidas de protección para reducir al mínimo la posibilidad y las repercusiones de incidentes como incendios, inundaciones, terremotos, explosiones, disturbios civiles, etc.
2) El sistema eléctrico del centro de cómputo debe contar con un sistema de UPS, así como de condiciones eléctricas acordes a las normas internacionales.
3) Las instalaciones del centro de cómputo se deben supervisar 24 horas al día. Esta supervisión puede ser realizada por medio de las cámaras de video, puertas de emergencia y ventanas, personas de vigilancia en los centros, o una combinación de lo antes nombrado.
4) Los operadores, administradores y visitantes frecuentes al centro de cómputo, deben ser capacitados en los procedimientos que deben seguir cuando se presente un evento de origen físico que afecte la continuidad en la operación normal del centro de cómputo.
5) Los equipos y dispositivos que son utilizados para soportar las funciones del negocio, deben estar en un área de acceso restringido y separadas del ambiente de las oficinas y puntos de atención.
6) Está totalmente prohibido fumar y consumir alimentos en el centro de cómputo.
7) Cuartos que contienen el cableado o el equipo de comunicaciones (armarios de cableado, cuartos de PBX, etc.) debe tener siempre con acceso restringido y solamente a personal autorizado.

5.6.4 SEGURIDAD DEL CABLEADO

1) Debe haber un monitoreo periódico sobre las redes de cableado estructurado de voz y datos y los gabinetes de cableado, para detectar, eliminar o prevenir el uso de dispositivos no autorizados conectados a los cables.
2) El Jefe de TI debe asegurar que todas las conexiones de red que existan en un lugar que no está siendo utilizado de manera permanente están deshabilitadas.
3) Los conductos de cableado de red deben ser protegidos contra interferencia o interrupción. Esto incluye evitar cableado en áreas públicas, segregación de cableado de energía para eliminar interferencia y el rotulado claro para la identificación de los equipos.
4) Los cuartos asignados para los gabinetes de cableado estructurado deben contar con acceso físico restringido y no se debe almacenar ningún tipo de material inflamable.

5.6.5 MANTENIMIENTO DE EQUIPOS

1) La Coordinación TIC's con el apoyo de la Presidencia, debe garantizar que el acceso al mantenimiento preventivo y/o correctivo de software o hardware es realizado por funcionarios debidamente autorizados e identificados. Ningún funcionario de CLINALTEC debe permitir la manipulación de equipos y/o software por personal que no esté identificado y autorizado por la Coordinación TIC's. Si el equipo debe ser sacado de las instalaciones para realizar las reparaciones, la confidencialidad e integridad de cualquier información debe ser garantizada.
2) Todos los recursos de TI (hardware y software) que soportan la operación de los procesos de la organización, así como la atención de los Clientes en los diferentes canales de servicio, deben contar con un contrato de mantenimiento preventivo y correctivo por parte del fabricante o proveedor.
3) En caso de presentarse un daño sobre algún elemento de trabajo por causas como: golpes, derrame de bebidas, elementos extraños, o alguna causa atribuible al usuario, el costo de la reparación o reposición debe estar a cargo del responsable del activo tecnológico.

5.6.6 PROTECCIÓN Y UBICACIÓN DE EQUIPOS

1) Para prevenir el acceso, la duplicación y la transmisión no autorizada de información confidencial, todas las impresoras y copiadoras, se deben situar en áreas seguras.

2) Todos los equipos tecnológicos de CLINALTEC deben ser ubicados o localizados de tal forma que se reduzca al mínimo los riesgos o amenazas. Esto incluye amenazas como hurto o vandalismo, fuego, explosión, humo, agentes químicos, pérdida de servicios de soporte como energía, comunicación, agua o cualquier otra amenaza física.

3) Los cuartos adyacentes a las instalaciones de procesamiento de información no se deben utilizar para propósitos que pueden implicar los altos riesgos (Ej. espacio de almacenaje, cuarto de servicio, cafeterías, etc.)

4) Fumar, beber y comer en instalaciones de procesamiento de información está terminantemente prohibido.

5) CLINALTEC debe asegurar que cualquier equipo de procesamiento de datos que haya contenido información privada o información confidencial y que vaya a ser reutilizado, experimente un proceso de limpieza lógica antes de ser utilizado nuevamente. El proceso de limpieza lógica debe consistir en la destrucción de la información que reside en el equipo y la validación del proceso, para asegurar que ningún dato se deja en el equipo o pueda ser recuperado.

6) CLINALTEC debe asegurar que para cualquier equipo de procesamiento de datos que haya contenido información privada o información confidencial y vaya a ser dado de baja, sus dispositivos de almacenamiento de información (disco duro, memoria RAM, memoria FLASH, etc.) sean destruidos físicamente antes de su disposición final.

5.6.7 SEGURIDAD DE EQUIPOS MÓVILES

1) Todo equipo de propiedad de CLINALTEC que esté fuera de las instalaciones de la Organización, no debe ser desatendido por su responsable en lugares públicos.

2) La Presidencia debe asegurar a través de pólizas de seguro las computadoras portátiles, dispositivos móviles como Tablets o Smartphones.

3) La Coordinación TIC’s debe velar porque los estándares de seguridad documentados dentro de la política se apliquen a todos los equipos y la información que en ellos se almacena, sin importar la localización de los mismos.

4) El jefe de Área del funcionario a quien le sea asignado un portátil, debe solicitar la compra e instalación de guayas de protección para los portátiles

5.6.8 RETIRO DE EQUIPOS DE LAS INSTALACIONES

1) En caso de retiro de un equipo de las instalaciones de CLINALTEC, se debe solicitar permiso (utilizando el formato establecido) a la Coordinación TIC’s y debe quedar el registro de la fecha y

hora de salida en el libro de seguridad, también debe registrarse el nombre del responsable a cargo del equipo.

5.6.9 SUMINISTROS DE EQUIPOS DE SOPORTE ENERGÉTICO

1) La Coordinación TIC's debe asegurarse que las fuentes de alimentación continuas (UPS) son utilizadas en los equipos que apoyan las operaciones de negocio críticas para facilitar la disponibilidad de los sistemas y su correcto apagado. Las UPS deben ser revisadas periódicamente para asegurar que tienen la capacidad adecuada y aprobada, de acuerdo con las recomendaciones del fabricante.

2) La Coordinación TIC's, en apoyo del departamento de servicios generales debe realizar un estudio anual de las cargas en los circuitos eléctricos, para que, en una eventual falla del suministro de energía eléctrica, la planta electica envíe los voltajes adecuados, para sostener el sistema de corriente ininterrumpido en la corporación.

5.6.10 POLÍTICA DE ESCRITORIO LIMPIO

1) Está totalmente prohibido el uso de celulares, cámaras, unidades de almacenamiento externo (USB, CDROM, DVD, etc.) en las estaciones de trabajo asignadas para el cumplimiento de las funciones.

2) La información clasificada confidencial que no esté siendo utilizada por personal autorizado, debe permanecer siempre bajo llave y no debe ser desatendida en ninguna ubicación no controlada.

3) Todos los funcionarios que tengan bajo su responsabilidad información confidencial, deben garantizar su almacenamiento bajo llave en las instalaciones de la Entidad.

5.6.11 POLÍTICA DE EQUIPOS DESATENDIDOS

1) Cuando un funcionario se retire temporalmente de su puesto de trabajo, debe hacer un logout de la sesión del aplicativo y activar el bloqueo del escritorio de trabajo del computador mediante la opción de protector de pantalla.

2) La opción de protector de pantalla de Windows debe configurarse con los siguientes parámetros:
   - Activar el protector de pantalla después de 3 minutos de inactividad del computador.
   - El desbloqueo requiere contraseña de red

3) Durante cualquier reubicación del espacio de trabajo de un empleado, el empleado debe asegurar que todos los activos de información están protegidos durante el proceso de reubicación. Esto incluye, pero no se limita a, el equipo y los archivos impresos.

4) Durante cualquier reubicación del espacio de trabajo del empleado, la información altamente sensible debe ser trasladada por el dueño de la información.

5.7 GESTIÓN DE COMUNICACIONES Y OPERACIONES: [ISO/IEC 27002:2015 A.12 - A.13]

Son sus objetivos:

- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.
- Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.
- Cada Propietario de la Información junto con el Responsable de Seguridad Informática y la Gerencia de Tecnología Informática, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS: [ISO/IEC 27002:2015 A.12.1]

Documentación de los procedimientos operativos: [ISO/IEC 27002:2015 A.12.1.1] Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad Informática.

Control de cambios en las operaciones: [ISO/IEC 27002:2015 A.12.1.2] Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El Responsable de Seguridad Informática controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan y evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Procedimientos de manejo de incidentes: Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

Separación de funciones: Se contempla la separación de la gestión o ejecución de tareas o áreas de responsabilidad, en la medida de que la misma reduzca el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.
En los casos en los que este método de control no pudiera cumplirse, se implementarán controles tales como el monitoreo de las actividades y/o la elaboración de registros de auditoría y control periódico de los mismos.

Separación entre instalaciones de desarrollo e instalaciones operativas: Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

Gestión de instalaciones externas: En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio que se incluirán en el contrato de tercerización.

PLANIFICACIÓN Y APROBACIÓN DE SISTEMAS

Planificación de la capacidad: La Gerencia de Tecnología Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuado.

Para ello tomará en cuenta además los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información de la Clínica para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

Aprobación del sistema: La Gerencia de Tecnología Informática establece criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.

PROTECCIÓN CONTRA SOFTWARE MALICIOSO: [ISO/IEC 27002:2015 A.12.2]

Controles contra software malicioso: [ISO/IEC 27002:2015 A.12.2.1] El Responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. La Gerencia de Tecnología Informática, o el personal designado por éste, implementará dichos controles.

El Responsable de Seguridad Informática desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Mantenimiento:

Resguardo de la información: La Gerencia de Tecnología Informática y el Responsable de Seguridad Informática junto a los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. Con base a ello, se definirá y documentará un esquema de resguardo de la información.

Registro de actividades del personal operativo: La Gerencia de Tecnología Informática asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

- Tiempos de inicio y cierre del sistema.
- Errores del sistema y medidas correctivas tomadas.
- Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas
- Ejecución de operaciones críticas
- Cambios a información crítica

Registro de fallas: La Gerencia de Tecnología Informática desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
Administración de la red: El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Clínica, contra el acceso no autorizado. La Gerencia de Tecnología Informática implementará dichos controles.

Administración y seguridad de los medios de almacenamiento:

Administración de medios informáticos removibles: La Gerencia de Tecnología Informática, con la asistencia del Responsable de Seguridad Informática, implementará procedimientos para la administración de medios informáticos removibles, como pendrive o memorias USB, cintas, discos, casetes e informes impresos.

Eliminación de medios de información: La Gerencia de Tecnología Informática, junto con el Responsable de Seguridad Informática definirá procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.

Procedimientos de manejo de la información: Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo a lo establecido en el capítulo “Clasificación y Control de Activos”.

Seguridad de la documentación del sistema: La documentación del sistema puede contener información sensible, por lo que se considerarán las medidas para su protección, de almacenar la documentación del sistema en forma segura y restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

- **INTERCAMBIOS DE INFORMACIÓN Y SOFTWARE**

Acuerdos de intercambio de información y software: Cuando se realicen acuerdos entre Clínicas para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de la Clínica y las consideraciones de seguridad sobre la misma.

Seguridad de los medios en tránsito: Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar la utilización de medios de transporte o servicios de mensajería confiable, suficiente embalaje para el envío y la adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas.

Seguridad del gobierno electrónico: El Responsable de Seguridad Informática verificará que los procedimientos de aprobación de Software del punto “Aprobación del Sistema” incluyan, para las aplicaciones de Gobierno Electrónico, los siguientes aspectos:

- Autenticación: Nivel de confianza recíproca suficiente sobre la identidad del usuario y la Clínica.
- Autorización: Niveles de Autorización adecuados para establecer disposiciones, emitir o firmar documentos clave, etc. Forma de comunicarlo al otro participante de la transacción electrónica.
- Procesos de oferta y contratación pública: Requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos.
- Trámites en línea: Confidencialidad, integridad y no repudio de los datos suministrados con respecto a trámites y presentaciones ante el Estado y confirmación de recepción.
- Verificación: Grado de verificación apropiado para constatar la información suministrada por los usuarios.
- Cierre de la transacción: Forma de interacción más adecuada para evitar fraudes.
- Protección a la duplicación: Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.

- No repudio: Manera de evitar que una entidad que haya enviado o recibido información alegue que no la envió o recibió.
- Responsabilidad: Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.

SEGURIDAD DEL CORREO ELECTRÓNICO

Riesgos de seguridad: Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

- La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.
- La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
- Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.
- La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.
- El impacto de un cambio en el medio de comunicación en los procesos de la Clínica.
- Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
- Las implicancias de la publicación externa de listados de personal, accesibles al público.
- El acceso de usuarios remotos a las cuentas de correo electrónico.
- El uso inadecuado por parte del personal.

Política de correo electrónico: El Responsable de Seguridad Informática junto con la Gerencia de Tecnología Informática definirá y documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

- Protección contra ataques al correo electrónico, por ejemplo, virus, intercepción, etc.
- Protección de archivos adjuntos de correo electrónico.
- Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos.
- Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.
- Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
- Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).
- Definición de los alcances del uso del correo electrónico por parte del personal de la Clínica.

NO ES PERMITIDO

Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes con datos sensibles que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes

que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

No es permitido cadenas de correos con datos personales que evidencien intercambio de los mismos de manera irresponsable o con fines no permitidos en la organización o que no sean válidos para dar formal cumplimiento con lo estipulado en la ley 1581 de protección de datos personales y que no estén alineados con la política interna de protección de datos personales de la Clínica CLINALTEC.

Utilizar la dirección de correo electrónico corporativo como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, TikTok, Instagram, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

El envío de archivos que contengan extensiones ejecutables, en ninguna circunstancia.

El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección respectiva y la Dirección de Tecnología.

El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que la clínica proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.

El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación de la Oficina respectiva de Comunicaciones, mercadeo o medios de comunicación y la autorización de la Dirección de Tecnología. Además, para terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre de la dependencia respectiva y/o Servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.

Toda información de la clínica generada con los diferentes programas computacionales (Ej. Office365, Project, Access, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables usando tecnologías como cifrado de datos, utilizando las características de seguridad que brindan las herramientas proporcionadas por el Área Tecnología e innovación. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la CLÍNICA INTERNACIONAL DE ALTA TECNOLOGÍA - CLINALTEC y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

POLÍTICA CONTRA CÓDIGOS MALICIOSOS - [ISO/IEC 27002:2015 A.12.2.1]

La CLÍNICA INTERNACIONAL DE ALTA TECNOLOGÍA - CLINALTEC establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, anti spam, antispyware, anti rootkits, anti RANSOMWARE, Cifradores y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red corporativa, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código

móvil y malicioso. Será responsabilidad del encargado de la seguridad informática y de la dirección de tecnología autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados en ninguna circunstancia, así como de su actualización permanente.

Así mismo, la CLÍNICA INTERNACIONAL DE ALTA TECNOLOGÍA - CLINALTEC define los siguientes lineamientos:

- No está permitido:
- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por LA CLÍNICA CLINALTEC.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.
- El uso de código móvil. Éste sólo podrá ser utilizado si opera de acuerdo con las políticas y normas de seguridad definidas y debidamente autorizado por la Dirección de Tecnología.

SEGURIDAD DE LOS SISTEMAS ELECTRÓNICOS DE OFICINA

Se controlarán los mecanismos de distribución y difusión tales como documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios o instalaciones postales, equipos de fax, etc.

Sistemas de acceso público: Se tomarán medidas para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada.

Otras formas de intercambio de información: Se implementarán normas, procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo.

DESARROLLO Y MANTENIMIENTO DE SISTEMAS: [ISO/IEC 27002:2015 A.14]

Son sus objetivos:

- Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.
- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
- Definir los métodos de protección de la información crítica o sensible.
- Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por la Clínica en donde residan los desarrollos mencionados.
- El Responsable de Seguridad Informática junto con el Propietario de la Información y el Área de Procesos, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El Responsable de Seguridad Informática, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el

Responsable de Seguridad Informática definirá junto con la Gerencia de Tecnología Informática, los métodos de encriptación a ser utilizados.

- **REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS: [ISO/IEC 27002:2015 A.14.1]**

Análisis y especificaciones de los requerimientos de seguridad: Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen. Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Seguridad en los sistemas de aplicación:

Validación de datos de entrada: Se definirá un procedimiento que, durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Controles de procesamiento interno: Se definirá un procedimiento para que, durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

Autenticación de mensajes: Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán controles criptográficos.

Validación de datos de salidas: Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

- Comprobaciones de la razonabilidad para probar si los datos de salida son coherentes.
- Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.
- Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.
- Procedimientos para responder a las pruebas de validación de salidas.
- Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

- **CONTROLES CRIPTOGRÁFICOS: [ISO/IEC 27002:2015 A.10.1]**

Se utilizarán sistemas y técnicas criptográficas para la protección de la información con base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

- **POLÍTICA DE UTILIZACIÓN DE CONTROLES CRIPTOGRÁFICOS: [ISO/IEC 27002:2015 A.10.1.1]**

Se utilizarán controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada, fuera del ámbito de la Clínica.

- Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad Informática.

Cifrado: Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el Responsable de Seguridad Informática, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

Firma digital: Se tomarán medidas para proteger la confidencialidad de las claves privadas. Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

Servicios de no repudio: Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

ADMINISTRACIÓN DE CLAVES: [ISO/IEC 27002:2015 A.10.1.2]

Protección de claves criptográficas: Se implementará un sistema de administración de claves criptográficas para respaldar su utilización por parte de la Clínica. Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada. Se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

Seguridad de los archivos del sistema: Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

Control del software operativo: Toda aplicación, desarrollada por la Clínica o por un tercero tendrá un único responsable designado formalmente por la Gerencia de Tecnología Informática.

Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrán acceder a los ambientes de producción.

La Gerencia de Tecnología Informática, propondrá para su aprobación por parte de la Gerencia General, la asignación de la función de “implementador” al personal de su área que considere adecuado.

Protección de los datos de prueba del sistema: Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos a tal efecto.

Control de cambios a datos operativos: La modificación, actualización o eliminación de los datos operativos serán realizadas a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos.

Control de acceso a las bibliotecas de programas fuentes: La Gerencia de Tecnología Informática, propondrá para su aprobación por parte de la Gerencia General la función de “administrador de programas fuentes” al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes.

SEGURIDAD DE LOS PROCESOS DE DESARROLLO Y SOPORTE: [ISO/IEC 27002:2015 A.14.2]

PROCEDIMIENTO DE CONTROL DE CAMBIOS: [ISO/IEC 27002:2015 A.14.2.2]

Se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Revisión técnica de los cambios en el sistema operativo: [ISO/IEC 27002:2015 A.14.2.3] Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Restricción del cambio de paquetes de software: [ISO/IEC 27002:2015 A.14.2.4] La modificación de paquetes de software suministrados por proveedores, previa autorización de la Gerencia de Tecnología Informática, deberá:

Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
Determinar la conveniencia de que la modificación sea efectuada por la Clínica, por el proveedor o por un tercero.

Evaluar el impacto que se produce si la Clínica se hace cargo del mantenimiento.
Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

CANALES OCULTOS Y CÓDIGO MALICIOSO: [ISO/IEC 27002:2015 A.14.2.6]

Se redactarán normas y procedimientos que incluyan:

Adquirir programas a proveedores acreditados o productos ya evaluados.
Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
Controlar el acceso y las modificaciones al código instalado.
Utilizar herramientas para la protección contra la infección del software con código malicioso.

DESARROLLO EXTERNO DE SOFTWARE: [ISO/IEC 27002:2015 A.14.2.7]

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

- Acuerdos de licencias, propiedad de código y derechos conferidos.
- Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
- Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.

- Verificación del cumplimiento de las condiciones de seguridad contempladas en los requerimientos de Seguridad en Contratos de Tercerización.
- Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

ADMINISTRACIÓN DE LA CONTINUIDAD DE LAS ACTIVIDADES DE LA CLÍNICA: [ISO/IEC 27002:2015 A.17]

Son sus objetivos:

- Minimizar los efectos de las posibles interrupciones de las actividades normales de la Clínica (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

- Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Maximizar la efectividad de las operaciones de contingencia de la Clínica con el establecimiento de planes que incluyan al menos las siguientes etapas:

- Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.
- Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
- Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal de la Clínica y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

El Responsable de Seguridad Informática participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia. Los Propietarios de la Información y el Responsable de Seguridad Informática cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la Clínica.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Clínica.

PROCESO DE LA ADMINISTRACIÓN DE LA CONTINUIDAD DE LA CLÍNICA: [ISO/IEC 27002:2015 A.17.1.1]

El CSI, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades de la Clínica.

Continuidad de las actividades y análisis de los impactos: Se establece la necesidad de contar con un Plan de Continuidad de las Actividades de la Clínica que contemple los siguientes puntos:

Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades.

Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación.

- **IDENTIFICAR LOS CONTROLES PREVENTIVOS**

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Responsable de Seguridad Informática, considerando todos los procesos de las actividades de la Clínica y no limitándose a las instalaciones de procesamiento de la información.

- **ELABORACIÓN E IMPLEMENTACIÓN DE LOS PLANES DE CONTINUIDAD DE LAS ACTIVIDADES DE LA CLÍNICA: [ISO/IEC 27002:2015 A.17.1.2]**

Los propietarios de procesos y recursos de información, con la asistencia del Responsable de Seguridad Informática, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Clínica. Estos procesos deberán ser propuestos por el CSI.

Marco para la planificación de la continuidad de las actividades de la Clínica: Se mantendrá un solo marco para los planes de continuidad de las actividades de la Clínica, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

- **ENSAYO, MANTENIMIENTO Y REEVALUACIÓN DE LOS PLANES DE CONTINUIDAD DE LA CLÍNICA: [ISO/IEC 27002:2015 A.17.1.3]**

El CSI establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.

5.9 CUMPLIMIENTO DE LOS REQUISITOS LEGALES

5.9.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE

1) Todos los requisitos legales, contractuales, o regulatorios que sean aplicables a la Organización, deben ser documentados y definidos por la Oficina Jurídica. Los requisitos y las responsabilidades específicas de controles u otras actividades relacionadas, con estas regulaciones legales, deben ser delegados a la unidad de negocio apropiada.

5.9.2 DERECHOS DE PROPIEDAD INTELECTUAL

- Todo el software instalado en las estaciones de trabajo y servidores de CLINALTEC debe ser licenciado y los usuarios deben cumplir con las leyes y las restricciones de derecho de autor definidos por el fabricante. Adicionalmente, todo el software instalado en los recursos informáticos de la Entidad debe ser aprobado por el Jefe de TI y el Oficial de Seguridad de la información. Cualquier software introducido en el ambiente de producción, debe ser analizado y aprobado por estas áreas.

- Está prohibido el almacenamiento y uso de archivos con extensiones .avi, .mp3, .mpg, .jpg los cuales corresponden a archivos de video, música, gráficos, juegos, etc. Que no estén debidamente licenciados por la Empresa.

- La instalación de software o el uso de información externa en los recursos informáticos de CLINALTEC debe ser previamente autorizada por la Presidencia y debe cumplir con los requerimientos legales que faculten su utilización.

- El software que reside en los computadores de CLINALTEC sólo podrá ser el autorizado por la Presidencia. No se podrá instalar en los computadores de La Empresa software que no esté registrado y autorizado.

- El Coordinador de TI de CLINALTEC realizará revisiones periódicas al software instalado en las estaciones de trabajo y eliminará sin previo aviso todos los aplicativos y archivos que no estén autorizados previamente. Los responsables de la instalación, descarga y/o uso de software que viole los acuerdos de licenciamiento serán sujetos de las acciones disciplinarias definidas por parte de la Presidencia.

- La Coordinación TIC's y el Oficial de Seguridad deben aprobar todo el shareware, freeware y software libre para ser usados en los recursos de cómputo de la Entidad con el fin de asegurar que en el software no esté presente código malicioso y/o que no cumpla con las necesidades de la Entidad o de seguridad.

- Las violaciones de los derechos o políticas de propiedad intelectual de la Entidad están sujetas a acciones disciplinarias.

- La compra o uso de software de terceros debe cumplir con los acuerdos de licenciamiento definidos por el fabricante. Estos acuerdos pueden detallar restricciones específicas del usuario (ej.: el número de las copias instaladas permitidas, número de máquinas donde es posible instalar el software o número de usuarios concurrentes que pueden conectarse al software). Los niveles de soporte al CLINALTEC (en sitio o por teléfono) se pueden también especificar dentro del acuerdo. El uso o copia del software comprado en un equipo adicional se prohíbe terminantemente.

5.9.3 PROPIEDAD INTELECTUAL

- Todos los desarrollos de productos realizados por funcionarios de la Organización, contratados o producidos bajo acuerdos que le asignen la propiedad intelectual del trabajo a CLINALTEC son de propiedad de CLINALTEC.

5.9.4 PREVENCIÓN DEL MAL USO DE INSTALACIONES DE PROCESAMIENTO DE DATOS

- El monitoreo de los sistemas de información y/o estaciones de trabajo se realizará exclusivamente por los organismos de control interno de la Organización y se debe llevar a cabo de acuerdo a las leyes y regulaciones locales.

- Los recursos de tecnología (hardware y software) son para uso exclusivo del negocio. El uso no adecuado de cualquier recurso de tecnología de la Entidad o para otros propósitos diferentes a los definidos por el negocio está prohibido. Cualquier actividad no autorizada debe ser reportada a la Presidencia.

- Los usuarios deben ser notificados, mediante mensajes escritos o a través de mensajes de alerta al obtener acceso a sistemas, que la actividad está siendo monitoreada.

5.9.5 PROTECCIÓN DE REGISTROS DE LA ENTIDAD

1) Los estándares para la recolección, custodia, manejo y destrucción de registros deben ser desarrollados para cualquier información cubierta por estatutos legales o regulatorios. El cronograma de retención para este tipo de información debe ser definido y divulgado. Dicho cronograma debe contener, sin limitar:

   - Tipo de información.
   - Estatutos reguladores relacionados.
   - Inventario de fuentes de este tipo de información.
   - Período de retención de registro.
   - Requerimientos apropiados de almacenaje y manejo.
   - Métodos apropiados de destrucción.
   - Cualquier requisito especial implementado que no esté definido en la política de seguridad de la Entidad.

2) Es responsabilidad del dueño de la información definir el cronograma de retención de cada registro documental.

5.9.6 REGULACIÓN DE CONTROLES CRIPTOGRÁFICOS

1) La seguridad criptográfica, incluyendo el uso de hardware o software, implementados en los sistemas corporativos deben cumplir con cualquier legislación local o internacional.

5.9.7 CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD

- Los jefes de servicios y departamentos deben llevar a cabo los procedimientos de escalamiento y reporte cuando se observa el incumplimiento o se genera una excepción de la política de seguridad de la Entidad.

- Los jefes de servicios y departamentos deben revisar regularmente los procesos y procedimientos dentro de su área para asegurar que las responsabilidades y deberes de seguridad se realizan

apropiadamente. Los resultados de esta revisión y las acciones correctivas deben ser documentados.

- El Oficial de Seguridad debe revisar el cumplimiento con las prácticas de seguridad de la Entidad. Las situaciones que dan como resultado el incumplimiento de las prácticas, deben ser reportadas a gerencia apropiada. Las actividades de revisión deben incluir el monitoreo operacional del cumplimiento, análisis individual del sistema, revisiones de terceros, pruebas de conformidad internas, y/o revisiones de los procedimientos.

- La violación deliberada de las políticas de seguridad de la información y/o del incumplimiento de regulaciones, será sancionada mediante un proceso disciplinario ejecutado por el área de Recursos Humanos para el caso de funcionarios de La Empresa o a través de contratos o procesos jurídicos en caso de terceros.

6. BIBLIOGRAFÍA

No Aplica