Universidad Nacional Experimental del Táchira

Políticas de Seguridad de la información

Organización: Clínica Todo EsSalud

Elaborado por:
Arturo Bernal CI: 19.925.695
Leydy Moreno CI: 24.743.325

San Cristóbal agosto de 2016

Clínica todo EsSalud

La clínica todo EsSalud en su afán de optimizar sus procesos y ofrecer un servicio de calidad, se compromete a salvaguardar de manera sistemática la seguridad de sus activos de información, pues los considera indispensables para la continuidad de sus procesos y actividades, es por ello que adoptará y aplicará las medidas necesarias para mantener la integridad confidencialidad y disponibilidad de su información.

Las políticas relacionadas con la seguridad de la información, pretenden concienciar a todas las personas involucradas directa o indirectamente con los procesos que constantemente se ejecutan en Todo EsSalud, dando a conocer, las mejoras prácticas para llevarlos a cabo, y por lo tanto, reducir el impacto que la materialización de un riesgo, pueda causar en un activo de la organización, tan sensible como es la información personal de un paciente, su historia clínica, la información de sus tarjetas de pago.

En tal sentido Todo EsSalud se compromete a:

1. Preservar las propiedades de la seguridad de la información.
2. Crear planes de formación continua para su personal.
3. Gestionar de manera sistemática sus riesgos.
4. Controlar los procesos y el intercambio de información con proveedores y clientes externos.
5. Considerar estándares de seguridad de la información enfocados al área de la salud o que se ajusten a sus necesidades como es el PCI DSS.

Política de escritorio limpio

1. Resumen ejecutivo

Sobre el escritorio no debe existir material sensible o confidencial que pueda poner en peligro algún activo de la clínica, de usarse dicho material durante la jornada laboral este debe ser guardado al final de la misma.

2. Alcance

Esta política aplica a todos y cada uno de los empleados y afiliados de la clínica Todo EsSalud.

3. Política

3.1 Los empleados están obligados a garantizar que toda la información sensible o confidencial de forma impresa o electrónica está segura en su área de trabajo ya sea al final del día o cuando por alguna razón se encuentre fuera durante un periodo prolongado.

3.2 Las estaciones de trabajo deben estar cerradas cuando no está ocupado el espacio de trabajo.

3.3 Las estaciones de trabajo se deben apagar por completo al final de la jornada de laboral.

3.4 Cualquier información restringida o sensible debe ser retirada de la mesa y guardada en un cajón del escritorio cuando no está ocupado y al final de la jornada de trabajo.

3.5 Gabinetes de archivos que contengan información sensible o restringidas deben mantenerse cerradas y bloqueadas cuando no estén en uso.

3.6 Las claves utilizadas para el acceso a la información restringida o sensible no debe dejarse sin vigilancia sobre el escritorio.

3.7 Las computadoras portátiles deben ser bloqueadas guardadas bajo llave en un cajón.

3.8 Las contraseñas no se pueden dejar en notas adhesivas o debajo de un ordenador, ni pueden ser dejados por escrito en un lugar accesible.

3.9 Debe ser removida inmediatamente de la impresora información restringida o sensible, si esta contiene dicha información.

3.10 Tras la eliminación de los documentos sensibles, estos deben ser triturados en los contenedores oficiales de fragmentación o se colocan en los contenedores de eliminación de bloqueos confidenciales.

3.11 Pizarras que contienen información sensible o restringida deben ser borradas.

3.12 Encerrar a los dispositivos informáticos portátiles tales como ordenadores portátiles y tabletas.

3.13 CD-ROM, DVD o unidades USB con información sensible deben ser guardadas en un cajón cerrado con llave.

4. Métricas de Cumplimiento

Todo EsSalud verificará el cumplimiento de esta política a través de diversos métodos, incluyendo, pero no limitado a, los videos de vigilancia, informes de la herramienta de negocios, auditorías internas y externas.

5. No cumplimiento

Los empleados que deliberadamente o por negligencia infrinjan en esta política serán objeto de medidas disciplinarias por parte de recursos humanos.

6. Estándares relacionados

Ninguno.

7. Histórico de Revisiones

Fecha de cambio	Responsable	Resumen de cambios
Julio 2016	Equipo de sistemas de Todo EsSalud	Nueva política

Política de correo electrónico

1. Resumen ejecutivo

Todo EsSalud ofrece a sus empleados una dirección de correo electrónico con la finalidad de facilitar el desempeño de sus funciones y permitir la comunicación entre departamentos, este método es ampliamente usado, pero es importante considerar los riesgos de privacidad y seguridad que podría traer su mal uso incluyendo problemas legales, esta política busca dar a conocer a los empleados los requisitos mínimos para el uso del correo electrónico dentro la organización.

2. Alcance

Esta política cubre el uso apropiado de cualquier correo electrónico enviado desde una dirección de correo electrónico de TodoEsSalud y se aplica a todos los empleados , proveedores y agentes que operan en nombre de TodoEsSalud.

3. Política

3.1 Todo el uso del correo electrónico debe estar en consonancia con las políticas y procedimientos de Todo EsSalud de conducta ética, la seguridad, el cumplimiento de las leyes y prácticas comerciales adecuadas aplicables.

3.2 La cuenta de correo electrónico de Todo EsSalud debe ser utilizado para fines relacionados con la organización.

3.3 Todos los datos de Todo EsSalud contenidos dentro de un mensaje de correo electrónico o un archivo adjunto se deben asegurar de acuerdo con la Norma de Protección de Datos.

3.4 El sistema de correo electrónico no será utilizado para la creación o distribución de mensajes perturbadores u ofensivos, incluyendo comentarios ofensivos sobre raza, género, color de pelo, discapacidad, edad, orientación sexual, la pornografía, las creencias y prácticas religiosas, políticas creencias, u origen nacional. Los empleados que reciben los correos electrónicos con este contenido desde cualquier empleado de Todo EsSalud deben informar de ello a su supervisor inmediato.

3.5 Los usuarios tienen prohibido el uso de sistemas de correo electrónico de terceros y servidores de almacenamiento, tales como Google, Yahoo, Hotmail y MSN, entre otros.

3.6 Todo el personal debe usar una firma estándar que incluye nombres y apellidos así como el departamento al cual pertenece y el número de teléfono con la extensión

---

Pedro Perez
Jefe de Recursos Humanos
Clínica Todo Es Salud C.A
Telf. 000000 Ext 111

3.7 Todo EsSalud puede controlar los mensajes sin previo aviso.

4. Métricas de Cumplimiento

El equipo de Todo EsSalud verificará el cumplimiento de esta política a través de auditorías y revisión del sistema de mensajes.

5. No cumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias, esta puede incluir la terminación del empleo de acuerdo a la gravedad del delito.

6. Estándares relacionados

Estándar de protección de Datos

7. Histórico de Revisiones

Fecha de cambio	Responsable	Resumen de cambios
Julio 2016	Equipo de sistemas de Todo EsSalud	Nueva política

Política de

1. Resumen ejecutivo

Todo

2. Alcance

Esta

3. Política

3.1 Todo el

4. Métricas de Cumplimiento

El equipo de Todo EsSalud.

5. No cumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias, esta puede incluir la terminación del empleo de acuerdo a la gravedad del delito.

6. Estándares relacionados

7. Histórico de Revisiones

Fecha de cambio	Responsable	Resumen de cambios
Julio 2016	Equipo de sistemas de Todo EsSalud	Nueva política