POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN IETS

INSTITUTO DE EVALUACIÓN TECNOLÓGICA EN SALUD (IETS)

Miembro de:

International Network of Agencies for Health Technology Assessment

Red de Evaluación de Tecnologías en Salud de las Américas

Centro asociado:

Versión: 1.

Número de páginas: 17.

Fecha: Julio de 2019.

El Instituto de Evaluación Tecnológica en Salud (IETS), es una corporación sin ánimo de lucro, de participación mixta y de carácter privado, con patrimonio propio, creado según lo estipulado en la Ley 1438 de 2011. Su misión es contribuir al desarrollo de mejores políticas públicas y prácticas asistenciales en salud, mediante la producción de información basada en evidencia, a través de la evaluación de tecnologías en salud y guías de práctica clínica, con rigor técnico, independencia y participación. Sus miembros fundadores son el Ministerio de Salud y Protección Social, el Departamento Administrativo de Ciencia, Tecnología e Innovación (Colciencias), el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (INVIMA), el Instituto Nacional de Salud (INS), la Asociación Colombiana de Facultades de Medicina (ASCOFAME) y la Asociación Colombiana de Sociedades Científicas.

Autores

May, Luciano. Ingeniero de Sistemas, M.Sc.(c) en Seguridad de la Información. Colaborador de la Unidad de Analítica del IETS.

Revisores

Espinosa, Oscar. Economista, M.Sc. en Ciencias-Estadística. *Citizen Data Scientist* Certificado. Coordinador de la Unidad de Analítica del IETS.

Barragan, Luz. Abogada

Fuentes de financiación

Instituto de Evaluación Tecnológica en Salud (IETS).

Conflictos de interés

Los autores declaran, bajo la metodología establecida por el Instituto de Evaluación Tecnológica en Salud (IETS), que no existe ningún conflicto de interés invalidante de tipo financiero, intelectual, de pertenencia o familiar que pueda afectar el desarrollo de esta herramienta computacional.

Derechos de autor

Citación

May, L. (2019). *Política de seguridad de la información IETS.* Bogotá D.C.: Instituto de Evaluación Tecnológica en Salud (IETS).

Correspondencia

Instituto de Evaluación Tecnológica en Salud (IETS)
Carrera 49A No. 91 – 91
Bogotá, D.C., Colombia
www.iets.org.co
contacto@iets.org.co

Contenido

1. OBJETIVO

El objetivo de esta política es garantizar que: i) la confidencialidad de los datos y activos de información estén protegidos contra la divulgación no autorizada; ii) los incidentes (violación de seguridad) sean informados con prontitud; y iii) la integridad de los activos de datos e información estén protegidos de modificaciones no autorizadas o accidentales. Esto en el marco de acción de la disponibilidad y accesibilidad a los sistemas de tecnologías de la información (TI), cuando los colaboradores o funcionarios del Instituto de Evaluación Tecnológica en Salud (IETS) lo requieran.

2. ALCANCE

La Política de Seguridad de la Información aplica a colaboradores o funcionarios, contratistas y practicantes del IETS, que tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la entidad.

3. COBERTURA DE LA POLÍTICA

Los equipos cubiertos por estas políticas incluyen:

Infraestructura de red: el equipo alojado internamente para proporcionar la red IT del IETS, incluidos servidores, gabinetes, racks, cables, conmutadores, enrutadores, puntos de acceso inalámbrico, cortafuegos, servidores proxy, sistemas y dispositivos de autenticación y sistemas de acceso remoto.

Computadoras de escritorio: computadoras personales (PC) suministradas o asignadas a los colaboradores para la realización de sus tareas.

Computadores portátiles: computadoras personales portátiles suministradas o asignadas a los colaboradores para la realización de sus diferentes actividades laborales.

Teléfonos móviles: dispositivos de comunicación digital suministrados a los colaboradores para el desempeño de sus funciones.

Teléfonos de escritorio: dispositivos de comunicación por voz conectados a la infraestructura de red, incluidos teléfonos de escritorio, teléfonos de conferencia (teléfonos estrella), adaptadores de telefonía analógica, teléfonos (inalámbricos), entre otros.

Medios portátiles: dispositivos de almacenamiento electrónico como DVD, CD-ROM, tarjetas de memoria y discos duros proporcionados a los colaboradores en el desempeño de sus funciones.

Asimismo, todos los medios informáticos utilizados en las salas de reuniones del IETS.

4. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para el Instituto de Evaluación Tecnológica en Salud IETS, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones estarán determinados por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, miembros y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del IETS
- Garantizar la continuidad del negocio frente a incidentes.

5. POLÍTICA INSTITUCIONAL

5.1. Seguridad de contraseñas

Siempre que sea técnicamente posible, todos los recursos de tecnología de la información deben estar protegidos mediante el uso de contraseñas seguras.

Todas las contraseñas creadas para su uso dentro de los equipos del IETS, deben cumplir con los requisitos de esta política.

5.1.1. Monitoreo y auditoría

El Área de Tecnologías de la Información y la Comunicación (TIC) se reserva el derecho de supervisar y auditar todo el uso de contraseñas dentro de los gestores de procesamiento de información sanitaria o de ciudadanos (en inglés *Health Security Environment*, HSE), para garantizar el cumplimiento de esta política e identificar cualquier contraseña débil que pueda comprometer la seguridad de los equipos, sistemas, aplicaciones o tecnologías de la información.

5.1.2. Contraseña estándar

Todas las contraseñas deben ser únicas y cumplir con el siguiente estándar:

5.1.2.1. Longitud de la contraseña

Todas las contraseñas deben tener un mínimo de ocho (8) caracteres de longitud. Si los sistemas existentes no son capaces de soportar tal número de caracteres, se debe usar la cantidad máxima de caracteres permitidos dentro del sistema.

5.1.2.2. Complejidad de la contraseña

Las contraseñas deben contener una combinación de letras (mayúsculas y minúsculas), números (0-9) y al menos un carácter especial (por ejemplo: ", £, $, %, ^, &, *, @, #, ?, !, €).

Las contraseñas no se deben dejar en blanco.

5.1.2.3. Seguridad de contraseña

Los usuarios deben evitar usar la misma contraseña para múltiples sistemas o propósitos.

Cada usuario es responsable de todas las actividades realizadas en cualquier dispositivo, sistema de información o aplicación mientras está conectado con su cuenta de acceso individual y contraseña.

Con la excepción de las cuentas de acceso genéricas / grupales, los usuarios solo deben usar cuentas de acceso de usuario y contraseñas que les haya sido asignadas.

Los usuarios deben asegurarse de que todas las contraseñas, excepto las utilizadas para las cuentas de acceso genérico / grupal, se mantengan confidenciales en todo momento y no se compartan con otras personas, incluidos sus compañeros de trabajo o terceros.

Los usuarios no deben escribir sus contraseñas en o cerca de su computadora. Sin embargo, en circunstancias excepcionales en las que se debe anotar una contraseña, la

contraseña debe almacenarse en un lugar seguro y bloqueado, que no sea fácilmente accesible para otros.

Los usuarios no deben enviar sus contraseñas dentro de los mensajes de correo electrónico a menos que el mensaje de correo electrónico esté encriptado.

Los usuarios deben cambiar sus contraseñas al menos cada ciento veinte (120) días o cuando se les indique.

Los usuarios que sospechen que su contraseña es conocida por otros deben cambiar su contraseña de inmediato.

Los usuarios no deben abusar de su propia contraseña ni de la contraseña de otros usuarios con el fin de elevar privilegios a su cuenta para acceso al dominio de red, por encima de aquellos que han sido autorizados por el administrador.

El usuario debe asegurarse de que todas las contraseñas predeterminadas que proporciona un proveedor para los nuevos dispositivos y sistemas HSE, se modifiquen en el momento de la instalación.

5.2. Comunicaciones electrónicas

5.2.1. Transferencia de archivos

Siempre que sea posible, todas las transferencias externas de información confidencial o restringida deben realizarse electrónicamente a través de canales seguros -es decir, *File Transfer Protocol* (FTP seguro), *Transport Layer Security* (TLS), *Virtual Private Network* (VPN), etc.- o correo electrónico encriptado.

5.2.2. Correo electrónico

El propósito principal del sistema de correo electrónico es promover la comunicación efectiva en asuntos comerciales del IETS. Los usuarios autorizados pueden tener acceso a servicios de correo electrónico sujetos a los requisitos de su función dentro de la organización.

Los usuarios deben respetar la privacidad de los demás en todo momento y solo usar las cuentas de correo electrónico que se les haya emitido.

Los usuarios que usan el sistema de correo electrónico para uso personal deben asegurarse de presentar sus comunicaciones de manera que el destinatario tenga claro que el correo electrónico es de carácter personal y no es una comunicación corporativa en nombre del IETS.

Los usuarios deben tener cuidado al usar su cuenta de correo electrónico institucional para enviar mensajes personales, en cuanto a que sus palabras o acciones no tengan de alguna manera, directa o indirecta, un impacto negativo en el IETS.

Por razones de seguridad, los usuarios que reciben regularmente información confidencial o restringida por el correo electrónico institucional, no deben reenviar estos mensajes a su cuenta de correo electrónico personal de otro dominio.

Los usuarios deben asegurarse de mantener sus mensajes de correo electrónico personales separados de sus mensajes de correo electrónico relacionados con los temas internos del IETS.

En circunstancias en las que es necesario transmitir información confidencial o restringida por correo electrónico, el remitente debe asegurarse de que se realicen las siguientes verificaciones antes de enviar la información:

1. El nombre y la dirección de correo electrónico de todos los destinatarios previstos son correctos;
2. El mensaje de correo electrónico está claramente marcado como "Privado y confidencial"; ver link https://support.google.com/mail/answer/7674059?co=GENIE.Platform%3DDesktop&hl=es-419
3. Solo se enviará la cantidad mínima de información confidencial o restringida necesaria para una función o funciones determinadas;
4. La contraseña utilizada para descifrar la información confidencial o restringida no debe enviarse junto con el mensaje de correo electrónico original.
5. Cuando sea práctico, comprobar que el destinatario o los destinatarios hayan recibido el mensaje de correo electrónico con la respectiva información (es decir, solicite un recibo de entrega o llame por teléfono a los destinatarios para confirmar la recepción).

El correo electrónico puede formar o variar un contrato de la misma manera que una carta escrita. Los usuarios deben tener cuidado al redactar un correo electrónico, por lo que no se puede interpretar como la formación o la variación de un contrato cuando esta no es la intención.

La cantidad de correo electrónico en la bandeja de entrada del usuario y en la carpeta de elementos enviados debe mantenerse al mínimo. Los correos electrónicos personales y archivos adjuntos que no son del objeto social del IETS se deben eliminar tan pronto como sea posible después de la recepción. La información confidencial y restringida que se ha recibido por correo electrónico no se debe almacenar permanentemente en el buzón de un usuario una vez que se ha leído. Donde sea práctico, la información debe ser transferida a una carpeta segura en un servidor del IETS y eliminada del buzón del usuario. Los usuarios también deben vaciar el contenido de la carpeta de elementos eliminados para garantizar que todas las copias locales de la información se hayan eliminado de su buzón. El correo

electrónico y los archivos adjuntos antiguos relacionados con el trabajo que ya no se requieren deben eliminarse, y los que se deben conservar deben archivarse o trasladarse a una carpeta personal en la computadora del usuario.

Durante los períodos de ausencia planificados, como pausas profesionales, vacaciones o en cursos de formación, los usuarios deben asegurarse de que, cuando sea práctico, su buzón se desvíe a uno de sus colegas para que no haya interrupciones en la prestación del servicio.

Durante los períodos de ausencia no planificados, como problemas de salud, o cuando un usuario se olvidó de desviar su buzón de correo a uno de sus colegas, se le puede permitir al administrador de la plataforma tecnológica acceder a su computadora para recuperar los mensajes de correo electrónico relacionados con el objeto social del IETS, con el fin de minimizar cualquier interrupción de las actividades misionales. En tales circunstancias, los Subdirectores deben respetar la privacidad del usuario y no acceder a documentos o correos electrónicos de naturaleza personal, a menos que existan condiciones convincentes que lo justifiquen (por ejemplo, la detección y prevención de fraude).

Los usuarios que se retiran laboralmente del IETS, deben asegurarse de enviar todos los mensajes de correo electrónico importantes relacionados con el objeto social a su jefe inmediato o compañeros de trabajo antes de irse, para que no haya interrupciones de las actividades misionales después de desvincularse. También, debe asegurarse de eliminar todos los mensajes de correo electrónico personales (es decir, mensajes de correo electrónico de naturaleza personal que no estén relacionados con el IETS) de su buzón, ya que no es posible obtener una copia de estos una vez que se ha desvinculado de la empresa.

5.2.3. Internet e intranet

El propósito principal de los servicios de intranet e Internet del IETS es proporcionar acceso a una valiosa herramienta comercial para facilitar la comunicación, el intercambio de información, la educación, el aprendizaje y la investigación misional.

Los usuarios autorizados pueden tener acceso a los servicios de Internet a través de la red del IETS, sujetos a los requisitos de su función dentro del instituto.

De acuerdo con el Estándar de filtro de contenido de Internet, cada usuario que tenga acceso a través de la red HSE, será asignado a uno o más grupos de acceso de usuarios de Internet, dependiendo de su función. El IETS filtra automáticamente el acceso a Internet a través de su red y bloquea el acceso a sitios web individuales o categorías de contenido de Internet que considera inapropiadas.

El acceso a Internet desde dispositivos inteligentes estará exento de los protocolos de filtrado de contenido de Internet de HSE estándar. Sin embargo, los usuarios de los

dispositivos inteligentes serán responsables de todas las conexiones de Internet realizadas desde su dispositivo inteligente.

La información confidencial o restringida sobre las prácticas y procedimientos comerciales del IETS o la información personal sobre clientes o empleados debe publicarse en el portal de Internet del IETS, www.iets.org.co.

Los usuarios deben recordar que al visitar un sitio de Internet, la dirección única de su dispositivo informático (es decir, la dirección IP) puede registrarse en los sitios de Internet que visitan para que se pueda identificar el IETS. Por lo tanto, cualquier actividad de Internet que realicen puede afectar a la organización.

El IETS no será responsable de ninguna pérdida financiera o material por parte de un usuario individual al acceder a Internet para uso personal.

Los usuarios deben saber que la información alojada en Internet no ofrece garantía de precisión, confiabilidad o autenticidad.

El Área TIC de la entidad se reserva el derecho de retirar temporalmente los servicios de Internet / Intranet o partes del servicio de Internet / Intranet por razones técnicas u operativas.

5.2.4. Redes sociales

Para efectos de bienestar, el IETS no tiene bloqueado el acceso a la mayoría de los sitios web de redes sociales. Sin embargo, estos podrían ser bloqueados según indicaciones de la Dirección Ejecutiva, cuando se considere pertinente.

La información confidencial o restringida sobre las prácticas y procedimientos comerciales del IETS o la información personal sobre clientes o empleados no debe publicarse ni debatirse en ningún sitio web de redes sociales.

5.3. Acceso remoto

Las conexiones de acceso remoto deben controlarse estrictamente y solo se otorgan a usuarios que cumplen al menos uno de los siguientes criterios:

1. Personal del IETS que ha sido aprobado por la Dirección Ejecutiva para trabajar desde casa (eventualmente).
2. Personal del IETS que ha sido aprobado por el órgano de coordinación y evaluación de teletrabajo.
3. Personal del IETS o contratistas cuyo rol les obliga a pasar una cantidad considerable de su tiempo fuera de la oficina o el lugar de trabajo.
4. Personal del IETS que es responsable de la administración, soporte o mantenimiento de la red de y / o sistemas de información.

5. Proveedores de servicios comerciales de terceros contratados por el IETS para proporcionar bienes y servicios (por ejemplo: soporte técnico, consultoría, etc.).

El personal del IETS o contratistas con permiso de acceso remoto solo deben acceder a las instalaciones de la red, los servicios y los sistemas de información que son necesarios para poder llevar a cabo las responsabilidades de su función específica.

El Área TIC se reserva el derecho de bloquear una solicitud de acceso remoto por motivos técnicos, operativos o de seguridad.

Toda la información confidencial y restringida, transmitida a través de una conexión de acceso remoto, debe cifrarse antes de la transmisión o enviarse a través de un túnel cifrado, excepto cuando la conexión remota forme parte directa de la red IETS.

5.3.1. Computadoras de acceso remoto

Todos los empleados del IETS que se conectan a la red institucional de forma remota deben hacerlo utilizando un dispositivo de computadora personal o de propiedad del IETS (por ejemplo, computadora de escritorio, computadora portátil, dispositivo de computadora móvil, etc.).

Todos los dispositivos informáticos que están conectados a la red IETS de forma remota deben tener instalado un software antivirus actualizado.

Cuando sea posible, la información confidencial y restringida no se debe almacenar en el computador remoto. En circunstancias que se considere necesario y aprobado por cualquier Subdirección, la información puede almacenarse en un dispositivo informático remoto siempre que esté encriptada.

5.3.2. Sesiones de acceso remoto

Cuando sea técnicamente factible, todas las sesiones de acceso remoto que están inactivas durante más de 10 minutos deben ser bloqueadas o cerradas automáticamente. Cuando esto no sea posible, se debe indicar a los usuarios que cierren manualmente o 'bloqueen' su dispositivo informático (utilizando las teclas Ctrl + Alt + Supr).

Todas las sesiones de acceso remoto deben ser monitoreadas y registradas.

5.3.3. Registro y administración de acceso remoto

Todas las solicitudes de acceso remoto deben realizarse a través del jefe inmediato del colaborador con aprobación de la Dirección Ejecutiva.

5.4. Escritorios y pantallas despejadas

Se requiere que los trabajadores se aseguren de que toda la información delicada / confidencial en forma impresa o electrónica esté segura en su área de trabajo al final del día, así como cuando se espera que se hayan ido por un período prolongado.

Las estaciones de trabajo deben estar bloqueadas cuando el espacio de trabajo está desocupado.

Las estaciones de trabajo deben estar completamente cerradas, al final del día de trabajo.

Cualquier información restringida o confidencial debe retirarse del escritorio y bloquearse en un cajón cuando el escritorio esté desocupado y al final del día de trabajo.

Los archivadores que contienen información restringida o confidencial deben mantenerse cerrados y bloqueados cuando no se usan o cuando no se atienden.

Las claves utilizadas para acceder a información restringida o confidencial no deben dejarse en un escritorio desatendido.

Los computadores portátiles deben quedar asegurados en un cajón o archivador.

Las contraseñas no se pueden dejar en notas adhesivas (*post it*) publicadas o debajo de una computadora, ni se pueden dejar escritas en una ubicación accesible-visible.

Las impresiones que contienen información restringida o sensible deben eliminarse inmediatamente del historial de la impresora.

Los documentos restringidos y / o confidenciales a eliminar, se deben triturar y desechar.

Se debe bloquear los dispositivos portátiles o móviles tales como computadoras portátiles y tabletas cuando no se estén usando.

Se debe tratar los dispositivos de almacenamiento masivo como unidades de *Compact Disc Read-Only Memory* (CD-ROM), *Digital Versatile Disc* (DVD) o *Universal Serial Bus* (USB) como sensibles y asegurarlos en un cajón con llave.

Se debe asegurar que los documentos confidenciales no queden en las bandejas de la impresora para que alguna persona equivocada los recoja.

5.5. Dispositivos móviles

Los usuarios solo pueden instalar programas corporativos que son esenciales para su función en sus dispositivos móviles.

Los usuarios deben reportar todos los dispositivos perdidos o robados a la subdirección de operaciones inmediatamente.

Si un usuario sospecha que se ha realizado un acceso no autorizado a los datos de la empresa a través de un dispositivo móvil, debe informar el incidente al área TIC del IETS.

Los usuarios no deben cargar software pirateado o contenido ilegal en sus dispositivos.

Las aplicaciones solo deben instalarse desde fuentes oficiales aprobadas por las tiendas App Store o Google Play Store. Se prohíbe la instalación de código de fuentes no confiables. Si no está seguro de sí una aplicación es de una fuente aprobada, póngase en contacto con el área TIC.

Los dispositivos deben mantenerse actualizados con los parches provistos por el fabricante o la red. Como mínimo, los parches deben revisarse semanalmente y aplicarse al menos una vez al mes.

Los dispositivos no deben estar conectados a una PC que no tenga la protección antimalware actualizada y habilitada y que no cumpla con la política corporativa.

Los usuarios deben tener cuidado al fusionar las cuentas de correo electrónico personal y laboral en sus dispositivos. Deben tener especial cuidado para garantizar que los datos de la empresa solo se envíen a través del sistema de correo electrónico corporativo. Si un usuario sospecha que los datos de la empresa se han enviado desde una cuenta de correo electrónico personal, ya sea en el texto del cuerpo o como un archivo adjunto, deben notificar al área TIC inmediatamente.

Los requisitos anteriores se comprobarán con regularidad y, en caso de que un dispositivo no cumpla con los requisitos, podría ocasionar la pérdida del acceso al correo electrónico, un bloqueo del dispositivo o, en casos especialmente graves, un borrado del dispositivo.

El colaborador es responsable de la copia de seguridad de sus propios datos personales y la empresa no aceptará ninguna responsabilidad por la pérdida de archivos debido a la eliminación de un dispositivo no compatible por razones de seguridad.

5.6. Protección del software

El IETS utiliza solo las copias con licencia de software comercial o software desarrollado internamente. El Área TIC del IETS mantendrá un registro de todo el software comercial, incluidas todas las licencias de software, para garantizar que se cumpla con las condiciones de la licencia y la legislación pertinente. Los usuarios no deben instalar software desarrollado externamente en los equipos del instituto, sin la aprobación previa del Área TIC.

Se recuerda a todos los usuarios que es un delito hacer o usar copias no autorizadas de software comercial y que el uso de estas licencias puede desencadenar una falta grave.

Los productos de software requeridos por cualquier Subdirección deben ser aprobados por el Área TIC. A menos que se indique lo contrario, todas las licencias y adquisiciones de

software serán realizadas a través de la jefatura jurídica, y los usuarios deberán seguir todas las instrucciones emitidas con respecto a programas o aplicaciones específicos.

El IETS minimizará los riesgos de los virus informáticos a través de la educación, buenas prácticas y procedimientos, la aplicación de un sólido software antivirus y asegurando que las políticas de firewall sigan las pautas nacionales apropiadas. Los usuarios deben informar de inmediato al Área TIC cualquier virus detectado o sospechoso -troyano, spyware o malware- en sus computadoras.

5.7. Virus y protección de software malicioso

Para proteger la infraestructura tecnológica del IETS de virus informáticos y otro software malicioso, no se debe abrir ningún documento o archivo electrónico de ninguna fuente fuera del IETS a menos que se haya escaneado primero para detectar virus conocidos y software malicioso. Este requisito cubre los archivos electrónicos en cualquier formato, incluidos los disquetes, CD-ROM, DVD y archivos adjuntos de correo electrónico.

El Área TIC garantizará que el software antivirus esté disponible en cada computadora de escritorio y portátil que esté conectada a la red del IETS y se encargará de la actualización regular de dicho antivirus. Debido a su naturaleza, es poco probable que las computadoras de escritorio y portátiles que no están regularmente conectados a la red IETS tengan protección antivirus completamente actualizada. Los usuarios de estos dispositivos informáticos deben ponerse en contacto el Área TIC del instituto al menos una vez al mes y actualizar su software de detección de virus manualmente.

El Área TIC, no es responsable de suministrar o actualizar el software de detección de virus en dispositivos informáticos, que no son propiedad ni están alquilados por el IETS.

Los usuarios que reciben un mensaje de advertencia de virus, deben enviarlo al Área TIC para determinar la autenticidad de la advertencia. Bajo ninguna circunstancia deben reenviarlo a otros usuarios.

5.8. Almacenamiento de información

El Área TIC del IETS garantiza que:

1. Toda la información confidencial o restringida del IETS o de clientes, se almacena en un servidor de red del instituto.
2. Todos los servidores del IETS que alojan sistemas de información críticos, aplicaciones, bases de datos, sistemas financieros y sistemas de gestión deben ubicarse dentro de las instalaciones de alojamiento central del IETS.

3. Otros servidores del IETS que alojan sistemas de información que procesan datos confidenciales o restringidos, también se encuentran en el sitio dentro de las instalaciones gestionadas por el Área TIC.

La información confidencial o restringida almacenada en los servidores del IETS, que no que no pertenece a un sistema de información institucional, debe mantenerse dentro de una carpeta segura a la que solo pueden acceder los usuarios autorizados para la misma.

Los servidores están reservados para el alojamiento / almacenamiento de sistemas e información relacionados con el objeto social del IETS únicamente. Los usuarios deben almacenar toda la información personal que no es del IETS en su dispositivo informático local.

Cuando la información confidencial, restringida o un sistema de información de propiedad del IETS se almacena / aloja en una computadora local o dispositivo de almacenamiento extraíble, el usuario del dispositivo y su administrador de línea deben asegurarse de que se implementen los siguientes controles.

1. Donde sea posible, la computadora o dispositivo de almacenamiento extraíble está protegido con contraseña (encriptada).
2. La información confidencial y restringida y / o la computadora o dispositivo de almacenamiento extraíble se codifican cuando sea posible.
3. Solo se almacena la cantidad mínima de información confidencial o restringida necesaria para una tarea específica en la computadora o dispositivo de almacenamiento extraíble;
4. La información confidencial y restringida se respalda regularmente, y las copias de seguridad se almacenan en un lugar seguro y no con la computadora o dispositivo extraíble;
5. La información confidencial y restringida se elimina de la computadora o dispositivo de almacenamiento extraíble cuando ya no es necesaria.

Bajo ninguna circunstancia se deben usar memorias USB no aprobadas (encriptadas o no) para transferir o almacenar sistemas de información del IETS o información confidencial o restringida de clientes.

Los dispositivos de almacenamiento extraíbles y las memorias USB cifradas aprobadas por el Área TIC, excepto las que se utilizan con fines de respaldo, no deben utilizarse para el almacenamiento a largo plazo de información confidencial o personal.

Las grabaciones fotográficas, de video y de audio tomadas con autorización de las partes como parte de consenso, evaluaciones, panel de expertos, o reuniones con clientes deben transferirse del dispositivo de grabación (es decir, cámara digital, cámara de video, teléfono móvil, grabadora, etc.) a un servidor o equipo autorizado del IETS tan pronto como sea posible. Cuando se completa la transferencia, se debe eliminar la grabación fotográfica, de video o de audio en el dispositivo de grabación. En el caso de que esto no se pueda llevar

a cabo de inmediato, el dispositivo de grabación debe bloquearse de forma segura cuando no esté en uso.

5.9. Informe de incidentes de seguridad

El objetivo de la investigación de incidentes de seguridad es identificar, investigar y resolver cualquier violación de seguridad informática sospechosa o real.

Un incidente de seguridad es un evento que puede resultar en:

- Integridad del sistema degradada.
- Pérdida de disponibilidad del sistema.
- Divulgación de información confidencial.
- Interrupción de la actividad.
- Pérdida financiera.
- Acción legal.
- Acceso no autorizado a las aplicaciones.
- Pérdida de datos.

Los incidentes deben notificarse al Área TIC del IETS. Todos los incidentes de seguridad que puedan tener un impacto en la conectividad serán informados de inmediato, por el usuario que identifica el hecho.

Todos los usuarios deben informar las violaciones de seguridad reales, o cualquier inquietud o sospecha sobre infracciones de seguridad, tan pronto como surjan.

Todos los incidentes de seguridad reales se registrarán formalmente, se categorizarán según la gravedad, y las acciones registradas por el Área TIC se informarán al Subdirector de Operaciones o a la Dirección Ejecutiva.

5.10. Recuperación de desastres y continuidad del negocio

Todos los datos críticos de la operación del IETS, se deberán replicar entre servidores en ubicaciones en la nube, de modo que, si los servidores en una ubicación dejan de estar disponibles, el acceso se cambia automáticamente a los servidores en otra ubicación.

Todos los datos se copiarán en repositorios para que los datos existan en tres lugares (servidor principal, servidor alterno y almacenamiento en la nube). El equipo informático crítico debe estar equipado con baterías de respaldo (UPS) para garantizar que no falle durante los cambios o las paradas de emergencia.

Para minimizar el riesgo de los sistemas de TI del IETS, los planes de recuperación ante desastres serán puestos en marcha para garantizar:

1. Identificación de sistemas informáticos críticos.
2. Identificación de áreas de mayor vulnerabilidad y priorización de usuarios clave y áreas de usuarios.
3. Acuerdo con los usuarios para identificar escenarios de desastre y qué niveles de recuperación ante desastres se requieren.
4. Desarrollo, documentación y prueba de planes de recuperación ante desastres, incluidas tareas de identificación, acuerdo de responsabilidades y definición de prioridades.

Los planes de recuperación cubren diferentes niveles de incidentes, incluida la pérdida del área clave de usuario dentro del edificio, pérdida de una parte clave de la infraestructura de la red informática y la pérdida de potencia de procesamiento.

Adicional a esto, los procedimientos de emergencia que cubren las acciones que deben tomarse en respuesta a un incidente (por ejemplo, alertar al personal de recuperación ante desastres), se encuentran publicados en la intranet institucional, así como en material impreso en la Oficina del Área TIC.

5.11. Circulación de los datos personales a través de correo electrónicos

En el correo electrónico puede figurar información diversa que puede ser considerada como datos de carácter personal, en la medida que ofrece información sobre una persona física identificable, como puede ser en la dirección del emisor y destinatario, el asunto del correo, la fecha y hora del correo, ya que permite establecer el momento en que se envía y llegar a establecer el lugar donde se encontraba esta persona, así como el cuerpo del mensaje, la firma y documentos adjuntos.

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la ley 1581 de 2012 (Sentencia C- 748 de 2011).

Por tanto, se debe advertir al área jurídica, los casos en que potencialmente se incluya datos de carácter personal y/o confidencial, en el contenido del correo electrónico.