Cleveland Clinic

Políticas y procedimientos de Recursos Humanos aplicables a toda la empresa

Asunto:	Empleados alcanzados:	Política N.º	Rev.
SEGURIDAD DE LA INFORMACIÓN	TODOS	HREW	2

OBJETIVO

El objetivo de esta política es establecer y comunicar a los empleados la dirección general de las iniciativas de seguridad de la información de Cleveland Clinic, en lo que respecta a la protección de toda la información confidencial, privada y restringida contra cualquier acceso no autorizado (sea intencional o accidental), publicación, modificación, o destrucción sin importar su formato (papel, electrónico/digital, etc.). Esta política se complementa con políticas, estándares, procedimientos y directrices incluidos en el Manual en Línea de Privacidad y Seguridad de la Información de Cleveland Clinic y en las publicaciones, recordatorios y/o manuales departamentales sobre Privacidad y Seguridad de la Información de Cleveland Clinic.

Todas las políticas, estándares, procedimientos y directrices en material de Seguridad de la información se rigen por la legislación/reglamentación federal/estatal, obligaciones contractuales, entes reguladores independientes o son parte de un enfoque de “buenas prácticas del sector” en materia de seguridad de la información.

POLÍTICA

Esta política de Seguridad de la información rige para todas las computadoras, sistemas en red y datos electrónicos en poder y/o bajo el control de Cleveland y/o todo sistema computarizado conectado a las redes de Cleveland Clinic. En el mismo sentido, esta política rige para todas las plataformas (sistemas operativos), todos los tamaños de computadoras (desde computadoras de mano a computadoras centrales) y sistemas de software (sean estos desarrollados por cuenta propia o adquiridos a terceros). La política abarca la información tratada por computadoras y/o redes de computadoras. Si bien este documento hace mención a la información por voz o en papel, no aborda de manera directa la seguridad de la información contenida en estos formatos. Si desea obtener información sobre la protección de la información contenida en papel, consulte la política 905 sobre Clases de información y sistemas.

FUNCIONES Y RESPONSABILIDADES

Funciones de los usuarios: toda la información en papel o electrónica que se almacene o transmita mediante los sistemas computarizados de Cleveland Clinic es propiedad de Cleveland Clinic y debe encontrarse protegida contra el acceso, la divulgación, la vulneración o la destrucción no autorizados. Todos quienes estén vinculados con Cleveland Clinic, sin importar su función (medico/a, empleado/a, contratista, consultor(a), trabajador(a) temporario/a, socio/a comercial, voluntario/a, etc.) y entren en contacto con información o sistemas informáticos de Cleveland Clinic, deben atenerse a las políticas de Seguridad de la información contenidas en el presente y en similares políticas, estándares, procedimientos y directrices en materia de Seguridad de la Información y/o Privacidad.

Funciones de los Departamentos: cada departamento de Cleveland Clinic tiene la responsabilidad de implementa esta y otras políticas afines mediante el empleo de los procesos, estándares y directrices establecidos por el Departamento de Seguridad de la Información de Cleveland Clinic. Esta responsabilidad incluye:

- Llevar un registro de los logros en materia de seguridad de la información y de las áreas a mejorar.
- Ayudar a identificar, clasificar y salvaguardar la información confidencial y restringida
- Establecer procedimientos para orientar, capacitar y actualizar al personal del departamento sobre las exigencias de esta y otras políticas afines
- Brindar información relacionada con la seguridad de la información, la confidencialidad y las violaciones a la privacidad dentro del departamento a las Oficinas de Seguridad y privacidad de Cleveland Clinic

Función del Departamento de Seguridad de la Información

El Departamento de Seguridad de la Información de Cleveland Clinic ("El Departamento") tiene la responsabilidad de establecer y preservar políticas, estándares, procedimientos y directrices en materia de seguridad de la información de aplicación en toda la empresa. El Departamento ofrece la dirección y capacidad técnica para brindar una certeza razonable de que la información de Cleveland Clinic se encuentra debidamente protegida.

El Departamento hace las veces de enlace entre todos los departamentos, divisiones e institutos de Cleveland Clinic en lo que concierne a seguridad de la información y es el punto de referencia para todas las actividades en materia de seguridad de la información que tienen lugar en Cleveland Clinic. El Departamento tiene a su cargo ejecutar evaluaciones de riesgo, diseñar planes de acción, evaluar productos de los proveedores, participar en proyectos de desarrollo, colaborar en la implementación de controles, coordinar las actividades de Recuperación ante Desastres Informáticos e investigar fallos en la seguridad de la información.

Todas las cuestiones y/o problemas en materia de seguridad de la información deben encausarse a través del Departamento de Seguridad de la Información. El empleo de consultores externos, equipos externos de respuesta ante emergencias informáticas, u otros proveedores externos está taxativamente prohibido a menos que hayan sido autorizados por el Departamento.

Coordinación de actividades descentralizadas

La Gestión de la Seguridad de Cleveland Clinic implica un esfuerzo centralizado y descentralizado al mismo tiempo; de acuerdo con el sitio, plataforma y/o aplicación, la responsabilidad por la gestión de la seguridad podrá ser centralizada, descentralizada o ambas. Se espera que quienes tengan a su cargo el respaldo o gestión descentralizados de determinados sistemas o aplicaciones en particular trabajen de manera conjunta con el Departamento de Seguridad de la Información, a fin de alinear políticas, estándares, procedimientos y directrices y mejorar los niveles de seguridad y privacidad.

DISPOSICIONES GENERALES

Principio de seguridad de la información

La información es un activo que, al igual que otros activos comerciales importantes, tiene valor para una organización y debe protegerse debidamente; el Departamento de Seguridad de la Información protege a la información de un sinnúmero de amenazas a fin de evitar violaciones a las reglamentaciones que afectan a los pacientes, garantizar la continuidad empresarial, minimizar el daño comercial y maximizar la rentabilidad y las oportunidades comerciales. La información representada en datos impresos, escritos, electrónicos y audiovisuales, entre otros formatos, sólo podrá compartirse, almacenarse y protegerse atendiendo a las salvaguardas pertinentes.

Salvaguardas razonables y adecuadas

La seguridad de la información se logra mediante la implementación una serie de controles administrativos, físicos y técnicos razonables y adecuados, los cuales incluyen las políticas, prácticas, procedimientos, estructuras organizativas, funciones de software y demás. El propósito de estos controles es garantizar que se alcancen los objetivos de seguridad específicos de la organización.

Propiedad de la información y derechos de acceso

Toda aplicación e información computarizada es desarrollada para unidades de trabajo diseñadas en función de Cleveland Clinic.
Las unidades de trabajo de Cleveland Clinic (por ejemplo, los sectores, los departamentos y los institutos) son los “Propietarios de los datos” en relación a las aplicaciones y la información computarizadas que hubieran desarrollado para sí. Es responsabilidad de los Propietarios de los datos garantizar la integridad de la información y determinar a quién se le permite acceder a la información. Cada unidad podrá designar al personal específico que asuma la función de Propietarios de los datos.

Resguardo de la información

El cuidado y protección (“resguardo”) de toda la Información de Cleveland Clinic es responsabilidad del empleado o persona autorizada que posea o utilice la información en un momento dado. Sin perjuicio de quien sea el Propietario de los datos o los medios empleados para obtener la información (cargas, descargas, acceso en línea normal, etcétera), el usuario o poseedor de la Información de Cleveland Clinic debe responder personalmente por su preservación de conformidad con esta política.

Clasificación de la información

A fin de respaldar el principio de acceso a la información en función de la “necesidad de saber”, Cleveland cuenta con un sistema de clasificación de la información. Este sistema de clasificación existe no sólo para proteger información que es esencial para los pacientes y para Cleveland Clinic sino también para determinar “quién” puede acceder a “qué” información dentro

de la estructura de Cleveland Clinic. Para obtener más información, consulte la Política de Clasificación de Datos 801CCHS.

Controles de acceso obligatorios

Los siguientes controles de acceso deben aplicarse en todos los sistemas computarizados e informáticos de Cleveland Clinic.

- **Sólo usuarios autorizados:** todas las PC no ofrecidas al público están reservadas al uso exclusivo de los usuarios autorizados por Cleveland Clinic. El uso no autorizado está terminantemente prohibido.
- **Identificación y autenticación:** todos los usuarios deben contar con identificación y contraseñas exclusivas para acceder a las redes, sistemas y/o aplicaciones sensibles de Cleveland Clinic
- **Identificaciones de usuario y contraseñas seguras**: las identificaciones de usuario y las contraseñas deben mantenerse en secreto y solo debe conocerlas el usuario; las contraseñas deben tener un largo considerable y ser difíciles de adivinar.
- **Administración de cuentas**: sólo el personal autorizado con funciones de seguridad está facultado a asignar y mantener cuentas de acceso restringido y privilegios asociados.
- **Acceso privilegiado**: el acceso privilegiado a menús de alto nivel como ‘’root’’, ‘’super user’’ o ‘’admin’’ está reservado exclusivamente a los administradores de sistemas.
- **Acceso de personal ajeno a Cleveland Clinic**: los contratistas, consultores, proveedores, etcétera, deben suscribir Acuerdos de confidencialidad y contar con la debida autorización de acceso otorgada por la dirección ejecutiva de Cleveland Clinic.
- **Acceso remoto**: el acceso remoto se otorgará a quienes ostenten una necesidad comercial válida, mediando la debida autorización. Idealmente, sólo se otorgará el acceso a los recursos que sean necesarios. Todos los usuarios remotos deben observar todas las políticas y procedimientos de acceso remoto.
- **Computadoras no atendidas**: todas las terminales de trabajo de Cleveland Clinic que se encuentren en sectores de acceso público o que contengan información sensible deben estar configuradas para desactivarse automáticamente transcurrido un periodo de tiempo razonable (la alternativa de un protector de pantalla autorizado es aceptable).
- **Computadoras no autorizadas**: las computadoras de propiedad particular que ingresen a las instalaciones de Cleveland Clinic deben ajustarse a las políticas de uso y conectividad de Cleveland Clinic. Todas las computadoras de este tipo deben tener instalados, además, los mismos niveles de control técnico (configuraciones, gestión de actualizaciones y antivirus).
- **Conexiones por fuera de la red (vía módem e inalámbricas)**: se prohíbe la conexión directa a las computadoras de Cleveland Clinic por medio de módems o conexiones inalámbricas que sorteen la conectividad y seguridad de la red.

- **Sistemas de redes inalámbricas y cableadas** La instauración de puntos de acceso inalámbricos y sistemas inalámbricos en las instalaciones de Cleveland Clinic sin la debida autorización está terminantemente prohibida. El uso no autorizado de puntos de acceso inalámbricos y sistemas inalámbricos para utilizar como puente o compartir las redes de Cleveland Clinic también está terminantemente prohibido.

Cumplimiento por parte de los proveedores

Los empleados de Cleveland Clinic deben adoptar las medidas razonables para poner a los proveedores en conocimiento de esta política de Seguridad de la Información de Cleveland Clinic y exigir a los proveedores su adhesión a todas las políticas, estándares y procedimientos que integran el programa de Seguridad de la Información de Cleveland Clinic.

Consideración de la seguridad de la información en las evaluaciones de desempeño de los empleados

La observancia de las políticas y procedimientos relacionados con la seguridad de la información es tenida en cuenta en todas las evaluaciones de desempeño de los empleados que correspondan (Evaluaciones de incorporaciones, Evaluaciones de mitad de año, Evaluaciones anuales de desempeño).

Control de conformidad, investigaciones y medidas disciplinarias

El control de conformidad se realizará de manera periódica a fin de ofrecer una certeza razonable de que las unidades organizativas se encuentran operando en concierto con las exigencias definidas en esta y otras políticas afines de seguridad de la información. La obtención, divulgación o discusión no autorizadas de toda información relacionada con las actividades comerciales de Cleveland Clinic, información médica sobre los pacientes, empleados actuales o anteriores y postulantes a puestos de trabajo, al igual que cualquier acto malicioso que destruya o atente contra cualquier tipo de información, será considerada grave y redundará en sanciones disciplinarias que llegan hasta el despido y la posible presentación de cargos penales. Las cuestiones disciplinarias resultantes de las violaciones a la seguridad de la información estarán a cargo de los directivos locales, quienes trabajarán en forma conjunta con Recursos Humanos.

Información de contacto

Todas las preguntas e inquietudes relacionadas con la seguridad de la información de Cleveland Clinic deberán dirigirse alguna de las siguientes alternativas:

- Director del Departamento de Seguridad de la Información de Cleveland Clinic: 216-738-4307
- Gerente del Departamento de Seguridad de Cleveland Clinic: 216-738-4320
- Mesa de ayuda de TI de Cleveland Clinic: 216-738-4357

OFICINA DE PUBLICACIÓN

Departamento de TI, Departamento de Seguridad de la Información y Oficina de Relaciones laborales, Recursos Humanos

REFERENCIAS DENTRO DE LA POLÍTICA

Medidas correctivas
900 Generalidades de la Seguridad de la Información
905 Clases de información y sistemas
925 Control de acceso
935 Uso aceptable de la información

CITAS

- Título 45 del Código de Regulaciones Federales. Artículo 142.308(a)(10)
- Título 45 del Código de Regulaciones Federales. Artículo 142.3088(a)(7)
- Título 45 del Código de Regulaciones Federales. Artículo 142.308(a)(12)