PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y CONTROLES DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo General:

Promover el desarrollo sostenible a partir de la modernización de la administración en el Centro Diagnóstico Automotor de Cúcuta, apoyados en el uso estratégico de las TIC, para contribuir en la construcción de una gestión más eficiente, transparente, participativo.

Objetivo Específicos:

Incorporar los lineamiento del Marco de Referencia de Arquitectura Empresarial y dominios del Gobierno de TI

Aplicar las políticas de seguridad de la información, implementando los controles para su adecuado funcionamiento.

Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del Sistema de gestión de seguridad de la información

Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

Crear todas las políticas de uso y servicios de redes para poder establecer permisos para la red,

Dominios de Gobierno de TI:

El CEDAC se proyecta lograr la alineación de los procesos con los esfuerzos en materia de uso y aprovechamiento de tecnologías de información es el foco del Gobierno de TI, para generar alineación entre los procesos del CEDAC y las TI, reflejando en “valor público”, que no es nada diferente a ofrecer a los ciudadanos servicios que mejoren su calidad de vida, protegiendo el medio ambiente y contribuyendo al crecimiento económico del país.

Con base en los establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones –MinTIC- en el CEDAC, se aplicarán los lineamientos que se establecen en el Marco de Referencia de Arquitectura Empresarial y uno de los dominios del marco es el de “Gobierno de TI”.

El marco de Referencia de AE, está estructurado en cuatro componentes:

Direccionamiento estratégico: Agrupa los principios generales del marco de referencia, dominios, ámbitos, elementos y lineamientos.

Instrumentos: Está compuesto de guías, estándares, mejores prácticas, normatividad que soportan o apoyan los dominios y los modelos de seguridad y privacidad de la información y de gestión estratégica de TI (IT4+).

Diseño conceptual: Está sustentado conceptualmente por las definiciones y los puntos de vista de arquitectura.

Implementación: Comprende un conjunto de indicadores sugeridos, la estructura organizacional y/o roles para estructurar la implementación de las acciones de cada dominio.

Dominios del Marco de Referencia de Arquitectura Empresarial:

Dominio de Estrategia: Tiene como objetivo apoyar la alineación de la estrategia de TI, con las estrategias organizacionales y sectoriales. Este dominio contribuye y facilita la estructuración de estrategias pertinentes para solucionar o responder a las necesidades de las instituciones, planear la gestión financiera y los recursos requeridos, definir los indicadores para el seguimiento a la implementación y ejecución de la estrategia de TI, diseñar el portafolio de planes, proyectos y servicios de TI, entre otros.

Dominio de Gobierno de TI: Tiene como objetivo dar lineamientos para implementar esquemas de gobernabilidad de TI en las entidades públicas y facilitar la incorporación de las políticas que permitan alinear los procesos de la institución con los procesos de TI y del sector. Para apoyar la construcción de un Gobierno TI es fundamental desarrollar un plan normativo y legal, las políticas organizacionales, los procesos de gestión de TI, el modelo de gobierno y los mecanismos de compras y contratación de la entidad.

Dominio de Información: Este dominio permite definir el diseño de los servicios de información, la gestión del ciclo de vida del dato, al análisis de información y el desarrollo de capacidades para el uso estratégico de la misma. Tiene como objetivo lograr que las instituciones públicas gestionen la información como un producto y/o servicio de calidad.

Dominio de sistemas de Información: Para soportar los procesos de las instituciones públicas es importante contar con sistemas de información que se conviertan en fuente única de datos útiles para apoyar o argumentar las decisiones corporativas. Este dominio permite planear, diseñar la arquitectura, el ciclo de vida, las aplicaciones, los soportes y la gestión de esos sistemas de información que facilitan y habilitan las dinámicas de una institución pública.

Dominio de servicios tecnológicos: La infraestructura tecnológica es la que soporta los sistemas y servicios de información en las instituciones, por eso es vital gestionarla con la

mayor eficiencia, optimización y transparencia. Este dominio le ayuda a las direcciones de tecnología y sistemas de información a gestionar los servicios tecnológicos que garanticen su disponibilidad y operación permanente, y que beneficien a todos los usuarios.

Dominio de uso y apropiación de TI: Al implementar todos los dominios que integran el Marco de Referencia de AE del Estado, se requiere hacer una adecuada gestión del cambio y de los grupos de interés, para desarrollar una cultura o comportamientos culturales que faciliten la adopción y uso de la tecnología, lo que es esencial para garantizar el resultado de las inversiones en TI y la transformación de las instituciones y sectores.

1. POLITICAS DE SEGURIDAD DE LA INFORMACION

1.1 Orientación de la Dirección para la Gestión de la Seguridad de la Información.

Objetivo. Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

Controles

1.1. Políticas para la Seguridad de la Información.

Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.

Como implementar este control

Se deben definir las Políticas de seguridad de la información para lo cual la entidad deberá apoyarse en la persona encargada del manejo de los sistemas y tecnología, sin embargo, todas estas políticas deberán ser revisadas y aprobadas por la Gerencia que en este caso es el más alto nivel de la entidad.

Las políticas de seguridad deben contener declaraciones muy específicas en cuanto a:

1) Definir claramente que es la seguridad de la información en el CEDAC y establecer cuáles serán los objetivos y alcances de estas políticas
2) Se deben asignar responsabilidades tanto de carácter general como responsabilidades específicas para poder gestionar el cumplimiento de las políticas de seguridad de la información

3) Se deben establecer procesos para manejar excepciones a alguna política en específico y quien podrá llevar a cabo dicho proceso

Cabe destacar que para poder establecer unas políticas de seguridad de la información completa se deberá tener claro conocimiento de todos los controles que se van a aplicar

1.2. Revisión de las Políticas para seguridad de la información.

Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.

Como implementar este control

Como se definió anteriormente cada política debe tener establecido quien será el responsable de su gestión, esto es de suma importancia para la implementación de este control ya que la persona responsable de la política será la encargada de su revisión, observar su desarrollo y evaluar la política. En su seguimiento de la política el responsable no solo deberá informar a la Gerencia si una política se cumple o no se cumple, también tendrá dentro de su responsabilidad observar si existen oportunidades de mejora que se puedan ir presentando debido a cambios que se puedan presentar en la organización, no obstante, las oportunidades de mejora no podrán ser aplicadas hasta tanto la alta Gerencia las haya revisado y aprobado.

2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

2.1 Organización Interna

Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del Sistema de gestión de seguridad de la información

Controles

2.1.1. Roles y Responsabilidades para la Seguridad de la Información

Se deben definir y asignar todas las responsabilidades de la seguridad de la información.

Como implementar este control

Para poder asignar responsabilidades se deben de tener definidas las políticas de seguridad de la información, la empresa debe de tener un inventario de activos actualizado para poder identificar las responsabilidades de cada uno de estos activos, para esto cabe aclarar que las personas responsables de un activo deberán ser personas capacitadas para su uso, sin embargo se pueden realizar orientaciones y capacitaciones detalladas a los responsables de los activos con el fin de que se lleve un mejor cumplimiento en la políticas de seguridad.

Los usuarios que se hayan definido como responsables en podrán delegar a otros la tarea del cumplimiento de la política de seguridad no obstante la responsabilidad seguirá siendo totalmente suya.

Para facilitar la definición de las responsabilidades se pueden seguir las siguientes indicaciones

1) Identificar y definir los activos en cada área y quiénes son sus usuarios o en su defecto quien es el jefe del área
2) Cuando se identifique los responsables de los activos se debe detallar y documentar las responsabilidades a este usuario
3) Para poder garantizar que las políticas de seguridad de la información asignadas a un responsable se cumplan la persona deberá ser competente en su área o haber recibido por parte de una persona competente y asignada por la alta gerencia una capacitación u orientaciones en el cumplimiento de dichas políticas

En algunas organizaciones se puede ver el caso que nombran a un único Responsables de seguridad de la información y este asume la responsabilidad total por el desarrollo, implementación y cumplimiento de la seguridad de la información y este a su vez puede nombrar un propietario para cada activo quien se convierte el responsable de su protección diaria, sin embargo esto es recomendable en el caso de que sean empresas pequeñas como es el caso del CEDAC.

2.1.2 Separación de Deberes.

Las Funciones y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.

Como implementar este control

A lo que este control se refiere es que cada persona o trabajador de la entidad deben tener definidas sus funciones y área de trabajo y tomar precauciones para que ninguna persona pueda acceder, modificar o usar un determinado activo que no le corresponde y sin autorización de su propietario o responsable, para una organización pequeña como lo

es el CEDAC se puede tener más bajo control este tipo de eventualidades manteniendo la restricción a áreas de personal no autorizado dando a conocer al personal que el uso de activos sin autorización puede acarrear problemas legales y que todo el tiempo están siendo monitoreados por el sistema cerrado de cámaras de la entidad.

2.1.3 Contacto con las autoridades.

Se debe mantener contactos apropiados con las autoridades pertinentes

Como implementar este control

La organización debe establecer unos procesos para definir cuándo y a través de qué forma se mantendrá contacto con las autoridades pertinentes, en el caso del CEDAC se debe establecer con cuales entidades se debe tener un especial contacto ya que al ser una empresa industrial y comercial del estado y también al ser supervisada por entidades gubernamentales debe presentar informes mensuales a estas entidades para evaluar que no se comentan irregularidades en el funcionamiento de la empresa, sin embargo toda esta información que se suministre a todas las entidades de control deben estar supervisadas por el responsable del sistema de gestión de seguridad de la información.

3. SEGURIDAD DE LOS RECURSOS HUMANOS.

3.1. Antes de asumir el empleo.

Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

Controles

3.1.1 Selección.

Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

Como implementar este control

El CEDAC al ser una empresa pública debe tener claramente definidos cuales son los antecedentes fiscales y parafiscales que debe solicitar a cada aspirante a un cargo, sin embargo, deben de tener en cuenta los siguientes aspectos

1) Además de todos los antecedentes de ley el CEDAC debe de exigir el diligenciamiento de la hoja de vida de la función pública que es de suma importancia, ya que al final de este formato el aspirante declara que no se encuentra inhabilitado bajo ninguna condición para ejercer cargos públicos.
2) Definir una persona encargada de verificar que la información presentada por el aspirante sea legitima, tanto antecedentes como certificaciones de estudios presentadas
3) Si el aspirante se presenta para un cargo en donde su responsabilidad tiene que ver con la seguridad de la información se debe demostrar que la persona es competente para este cargo.
4) Cada personal contratado se deberá incluir dentro de su contrato una clausula en la cual se deje claro la confidencialidad de los datos personales y de la entidad.

3.2. Términos y condiciones del empleo.

Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.

Como implementar este control

La empresa debe tener identificados cuales empleados o contratistas poseen acceso a información confidencial de la entidad los cuales deben firmar un acuerdo de confidencialidad y no divulgación que se ajuste a todos los términos legales vigentes esto se claramente se debe firmar antes de que puedan tener acceso a la información.

Todas las responsabilidades y los roles que tengan que ver con la seguridad de la información se deben de comunicar a la persona a contratar durante el proceso de vinculación y posteriormente en el proceso de inducción.

3.3 Durante la ejecución del empleo.

Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

Controles

3.3.1 Responsabilidades de la Dirección.

La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.

Como implementar este control

La dirección tiene una gran responsabilidad ya que debe de asegurar que las políticas de seguridad de la información y procedimientos establecidos sean cumplidos por todo el personal tanto empleados de planta como contratistas

La alta dirección debe informar desde el mismo momento de la vinculación las responsabilidades y funciones de seguridad de la información a cada empleado y contratista, no obstante si el empleado ya lleva tiempo en su cargo mucho antes de la implementación de las políticas de seguridad de la información, la alta Gerencia garantizar mediante orientaciones o capacitación al personal sus responsabilidades en la seguridad de la información y hacer firmar a estos un acta de que recibieron como constancia dichas directrices.

Todas estas capacitaciones y orientaciones suministradas al personal deben ir encaminadas a motivarlos para el cumplimiento de las políticas de seguridad de la información y en ningún momento se trata de intimidarlos en la ejecución de sus funciones.

3.1.2 Toma de conciencia, educación y formación de la Seguridad de la Información.

Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

Como implementar este control

Para el cumplimiento de este control la alta gerencia del CEDAC puede recurrir a capacitaciones de sensibilización y toma de conciencia, las cuales vayan encaminadas a que los empleados entiendan la importancia de la seguridad de la información y los motive a cumplir con sus responsabilidades asignadas a la seguridad informática.

Es importante que los empleados no solo tomen conciencia sino también tomen sentido de pertenencia por la entidad y comprendan el impacto positivo que la seguridad de la información trae para la entidad.

3.1.3 Proceso disciplinario.

Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

Como implementar este control

La empresa con el apoyo de los asesores jurídicos debe redactar todo el proceso disciplinario, el cual solo se iniciara si se verifica que ha existido una violación de alguna de las políticas de seguridad de la información, este tratamiento que se le dará al empleado o empleados de los cuales se sospeche que han cometido una falta referente a la seguridad de la información y dicho tratamiento debe ser imparcial y bajo los términos de ley que deben estar claramente identificados en el proceso disciplinario.

Dentro del proceso disciplinario la empresa puede incluir unos incentivos para los empleados que se destaquen en el cumplimiento de las políticas de seguridad informática

3.1.4Terminación y cambio de empleo.

Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

Control

3.1.4.1 Terminación o cambio de responsabilidades de empleo.

Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.

Como implementar este control

La empresa dentro del contrato del empleado o contratista debe incluir las responsabilidades que continúan aun después de la terminación del contrato y por cuanto tiempo dichas responsabilidades estarán vigentes, pero no solo si el contrato es terminado también se debe de informar las responsabilidades que siguen vigentes aun si el empleado cambia de cargo en la empresa ya sea por ejemplo por un ascenso, aunque el empleado ahora tendrá unas responsabilidades nuevas hasta no empalmar talmente con la persona que asumirá su anterior cargo dicho empleado no podrá hacer a un lado las responsabilidades que antes tenia

En muchas empresas todo el proceso de contratación, inicio, terminación y cambio de contratos es llevado a cabo por el área de recursos humanos, sin embargo en el caso del CEDAC este proceso es llevado a cabo por el área de secretaria general con el apoyo de los asesores jurídicos, es decir que esta área tendrá la obligación de informar todo claramente al empleado.

4. GESTIÓN DE ACTIVOS.

4.1 Responsabilidad por los Activos.

Objetivo. Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.

Controles

4.1.1 Inventario de Activos

Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

Como implementar este control

La empresa debe identificar cada uno de los activos asociados con la información, creando todo un listado de dichos activos los cuales pueden incluir los siguientes aspectos

1) Código que se le dará al activo
2) Nombre del activo
3) Ubicación del activo
4) Fecha de ingreso
5) Propietario del activo

Como mínimo debe contener esta información si la empresa considera importante introducir algún otro dato del activo en el inventario lo puede realizar, es importante recalcar que el inventario debe estar siempre actualizado y alineado con otros inventarios que posea la empresa.

En una empresa como el CEDAC que es del orden público es de suma importancia que se tenga un buen inventario para poder gestionar los activos ya que en caso de una visita por parte de entes de control que deseen conocer el estado y ubicación de los activos, lo puedan realizar mediante su inventario.

4.1.2 Propiedad de los activos.

Los activos mantenidos en el inventario deben ser propios.

Como implementar este control.

En el CEDAC todos los activos pertenecen obviamente a la empresa sin embargo a lo que este control se refiere como propietario, es a la persona a la cual se le asignara la responsabilidad del activo, este responsable al recibir el activo que estará a su cargo se le debe informar la forma en que lo debe recibir, es decir lo que él debe verificar al momento

de recibir el activo ya que al momento de entregar este activo se verificaran las condiciones en que se entregó, dentro de lo que debe revisar el nuevo propietario esta

1) Que el activo se encuentre correctamente inventariado
2) Que protecciones posee el activo
3) Que restricciones posee este activo
4) En qué condiciones físicas y de funcionamiento se recibe el activo

Cabe resaltar que el hecho de que la persona que ahora es propietaria de un activo no quiere decir que lo puede manipular a su antojo o moverlo como si fuese personal.

4.1.3. Uso Aceptable de los Activos

Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

Como implementar este control

Esto más que un control, se trata de tomar conciencia en el uso adecuado de los activos, si bien la empresa ha definido unas políticas de seguridad de la información y ha designado una responsabilidades bien definidas a los propietarios de los activos, se deben de seguir con sentido de pertenecía pensando siempre en el impacto positivo que esto genera al CEDAC.

4.1.4 Devolución de Activos.

Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

Como implementar este control

Cuando se dé por terminado un contrato o cuando un empleado decida voluntariamente renunciar al cargo que venía desempeñando y este fuese propietario de un activo, este activo debe de ser entregado de la misma forma y en el mismo estado en que se recibió, para esto el responsable de recibir el activo debe apoyarse en el inventario de activos, para poder saber en qué condiciones se entregó.

No solo basta con saber en qué condiciones físicas se entregar el activo el responsable de recibir el activo debe verificar su funcionamiento y si se manejaba información en dicho activo que la misma no se haya borrado y se encuentre disponible sin contraseñas ni algún método de encriptamiento.

4.1.5 Clasificación de la Información

Objetivo. Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.

Controles

4.1.5.1. Clasificación de la Información.

La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Como implementar este control

El CEDAC maneja mucha información referente a clientes, resultados de revisión, proveedores, contratación entre otras, sin embargo no toda la información posee la misma importancia existe información que es muy confidencial y podría causar un impacto significativo a corto plaza si se segara a divulgar, por lo cual al crear un esquema de clasificación de la confidencialidad de la información se pueden tener en cuenta cuatro niveles

1) Al divulgar la información no se causa daño a la organización ni a corto ni a largo plazo
2) La divulgación de la información causa inconvenientes menores de operación
3) La divulgación de la información causa un impacto significativo a corto plazo afectando las operaciones y objetivos de la empresa
4) La divulgación de la información tiene un serio impacto a largo plazo en los objetivos estratégicos e incluso puede poder en riesgo la supervivencia de la entidad

Dentro de la matriz de clasificación de la información se deberá indicar también el valor de los activos dependiendo que tan sensibles y críticos sean para la empresa desde el punto de vista de la confidencialidad, integridad y disponibilidad, la entidad podrá nombrar cada nivel de clasificación.

4.1.6 Etiquetado de la Información.

Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Como implementar este control

El etiquetado de la información deberá abarcar la información y sus activos relacionados en formatos físicos y electrónicos, como la empresa ya debía haber realizado la clasificación de la información, dentro de estas etiquetas se debe ver reflejado dicho esquema y deben ser de fácil reconocimiento.

Este etiquetado es de suma importancia para los procesos de intercambio de información, ya que se tiene con claridad cual información es confidencial y que el cuidado de su divulgación es crítico.

4.1.7 Manejo de Activos.

Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Como implementar este control

El CEDAC debe elaborar los procedimientos para el correcto manejo, procesamiento de los activos de información los cuales deben ser coherentes de acuerdo al nivel de clasificación que la empresa le ha otorgado

Se pueden tomar en cuenta los siguientes puntos

1) Que restricciones de acceso tendrá el activo
2) Mantener un registro formal de los receptores autorizados de los activos
3) Copias ya sean temporales o permanentes de la información de acuerdo a el nivel de clasificación
4) Seguir las indicaciones de los fabricantes de los activos para su correcto almacenamiento

5. MANEJO DE MEDIOS DE SOPORTE.

Objetivo. Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.

Controles

5.1 Gestión de medios de Soporte Removibles.

Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.

Como implementar este control

En el CEDAC se maneja tres discos duros extraíbles los cuales guardan copias de seguridad de la información de las revisiones, contabilidad y gestión de calidad y para estos se deben establecer unos procedimientos para su correcto almacenamiento, protección y evitar que se pueda perder la información allí almacenada, también se puede implementar dentro de los procedimientos métodos criptográficos para aplicar a estos medios removibles y así mitigar también el riesgo de que la información pueda ser copiada por personal no autorizado.

Se debe llevar un registro de la fecha, hora y personal que guarda las copias de seguridad en el dispositivo, para mantener un rastro de auditoria, cabe resaltar que no solo basta con realizar copias y guardarlas en los dispositivos se debe de crear un procedimiento para verificar la integridad y disponibilidad de la información guardada y el correcto funcionamiento de los dispositivos removibles.

5.2 Disposición de los medios de soporte.

Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.

Como implementar este control

Como se mencionó en el control inmediatamente anterior los dispositivos que maneja el CEDAC son tres discos duros extraíbles con información de gran importancia, para poder salvaguardar esta información mitigando el riesgo de que se pierda por un uso inadecuado de los dispositivos, se deben establecer procedimientos para su almacenamiento y manipulación, asignando solamente un responsable de estos procesos y llevando un registro de cuando se usa, que se almaceno, con el fin de poder llevar un rastros de auditoria.

5.3 Transferencia de medios de soporte físicos.

Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

Como implementar este control

En caso del que el CEDAC requiera enviar información ya sea física o mediante medios magnéticos se deben establecer procedimientos para garantizar que la información enviada llegue correctamente a su destino, para esto se pueden tener en cuenta los siguientes aspectos:

1) Cuando la información se envía dentro de la misma ciudad el CEDAC debe garantizar el correcto embalaje de la información para protegerla de factores

medioambientales que puedan dañarla y el mensajero del CEDAC debe llevar consigo un registro de a quién debe entregar esta información y que la persona que recibe firme para demostrar que la información se entregó correctamente.

2) Cuando la información se deba enviar a otras ciudades, es recomendable que la empresa utilice servicios de correo certificado, en los cuales siempre garantiza que el correo sea recibido en el lugar indicado y quien lo recibe, de lo contrario el paquete será devuelto a las instalaciones del CEDAC.

Como recomendación se puede anotar que cuando la información que se envía sea en medios magnéticos y sea información de carácter confidencial, se pueden tomar precauciones como cifrado de datos o sellos de seguridad que garantice que la información no fue abierta antes de llegar a su destinatario final.

6. CONTROL DE ACCESO.

6.1 Requisitos del Negocio para Control de Acceso

Objetivo. Limitar el acceso a información y a instalaciones de procesamiento de información.

Controles

Política de Control de Acceso.

Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

Como implementar este control

En este control el CEDAC debe de tener en cuenta tanto los controles de acceso lógicos como físicos para implementar correctamente las políticas para las cuales se debería tener en cuenta lo siguiente.

1) Uso de usuarios y contraseñas para el acceso a la información
2) Privilegios de acceso para los usuarios del sistema
3) Políticas para la divulgación y autorización de la información
4) Restricción de acceso a personal no autorizado a lugares donde se maneja información importante como área de servidores y redes.
5) Retiro de los derechos de acceso o privilegios a usuarios que ya no la requieran o que ya no hagan parte de la empresa

Cuando se implementan este tipo de políticas es preferible basarlas en las premisas, es decir; todo está prohibido a menos de que se permita expresamente.

6.2 Acceso a redes y a servicios en red.

Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

Como implementar este control

El CEDAC debe crear todas las políticas de uso y servicios de redes para poder establecer permisos para la red, en esta política se puede considerar los siguientes puntos:

1) Establecer con que servicios de red y aplicaciones de red cuenta la empresa
2) Determinar quiénes pueden tener acceso a la red y a que servicios
3) Controles que se tomaran para proteger los accesos a la red
4) Si se necesitan hacer conexiones remotas para soporte como se contrlaran y quienes estarán autorizados para usarlas
5) Como monitorearan la red de la empresa

7. GESTIÓN DE ACCESO DE USUARIOS.

Objetivo. Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.

Controles

7.1 Registro y cancelación del registro de usuarios.

Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.

Como implementar este control

El CEDAC debe gestionar la identificación de usuarios mediante el uso de nombre y claves de usuarios únicas para cada responsable que usa la red, sin embargo siempre que un usuario ya no haga parte de la entidad se debe proceder inmediatamente a la cancelación de su identificación o también si los usuarios no estarán en la entidad por un periodo como por ejemplo vacaciones, la identificación puede ser deshabilitada y habilitada nuevamente cuando el empleado se reintegre a sus actividades.

7.2 Suministro de acceso de usuarios.

Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.

Como implementar este control

El CEDAC al realizar el proceso de contratación ha debido explicar claramente a sus empleados las responsabilidades de seguridad informática como ya se mencionó anteriormente, sin embargo, cuando un usuario deba tener acceso a la red para cumplir con sus funciones a este se le debe otorgar un usuario con los privilegios que la empresa considere necesarios para cumplir con sus funciones.

En esto la empresa debe considerar lo siguiente:

1) Los usuarios y contraseñas deben ser privados e intransferibles
2) Verificar muy bien el nivel de acceso que se le dara al usuario y que son coherentes con la funciones que necesita realizar.
3) Verificar frecuentemente los derechos de acceso de los usuarios del sistema.

7.3 Gestión de derechos de acceso privilegiado.

Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.

Como implementar este control

Este control es muy importante para la empresa ya que lo que se debe realizar para cumplir con el es determinar los usuarios que podrán tener accesos privilegiados a los sistemas del CEDAC. Estos usuarios al poseer un acceso privilegiado también tienen una gran responsabilidad en la seguridad de la información de la empresa ya que serán los usuarios que posean un acceso mas a fondo de la información de la entidad para este control se puede considerar:

1) Que derechos de acceso privilegiado se otorgaran y a que sistemas de la empresa
2) Porque se le asigna derechos de acceso privilegiado a un usuario
3) El usuario al cual se le asignen estos derechos deben ser usuarios competentes e idóneos para las funciones que se le asignan
4) Recordar muy bien las responsabilidades que implica ser un usuario con acceso privilegiado

7.4 Gestión de información de autenticación secreta de usuarios.

La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.

Como implementar este control

Aunque en el CEDAC no se manejan lo que son autenticaciones secretas para los usuarios es importante considerar este control ya que en caso de que en alguno de sus sistemas lo quieran realizar sepan las consideraciones a tener para poder cumplir con este control que son:

1) Los usuarios con autenticaciones secretas deben de firmar una cláusula de confidencialidad para mantener secretas la información que este usuario este manejando

Un tipo de autenticación secreta podría ser el ingreso a sistemas de la entidad mediante tokens o tarjetas inteligentes las cuales poseen una clave secreta de autenticación

7.5 Revisión de los derechos de acceso de usuarios.

Los propietarios de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares

Como implementar este control

En este punto lo que debe de realizar la empresa es constantemente verificar que los derechos de acceso son los adecuados considerando lo siguiente

1) Se debe establecer cada cuanto tiempo se realizara la revisión de los derechos de acceso de los usuarios
2) Los derechos de acceso a usuarios se deben reasignar cuando se cambie de un rol a otro dentro de la empresa
3) Los cambios a usuarios privilegiados se deben de registrar para revisión periódica.

7.6 Cancelación o ajuste de los derechos de acceso.

Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.

Como implementar este control

Como se explicó anteriormente cada vez que un usuario del sistema sea retirado de la organización o cambie su rol dentro de ella misma, se debe cancelar o modificar sus privilegios de acceso al sistema ya sean físicos o lógicos, los cuales deberán ahora ser acordes a sus nuevas funciones, sin embargo, si el empleado se va a retirar, el proceso de terminación o ajuste debería comenzar antes de que el empleado termine su proceso de retiro.

8. RESPONSABILIDADES DE LOS USUARIOS.

Objetivo. Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.

Controles

8.1 Uso de información secreta para autenticación

Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.

Como implementar este control

Para el cumplimiento de este control el CEDAC debe considerar la realización de capacitaciones en las cuales se concientice a los empleados y contratistas en el uso adecuado de las contraseñas como por ejemplo:

1) Las contraseñas son personales e intransferibles
2) No tenerlas anotadas en papel, o en el escritorio o en algún otro medio a menos de que este sea seguro y no esté al disponible para ninguna otra persona más que para el dueño de esta contraseña.
3) Cambiar la contraseña cada determinado periodo de tiempo o cada vez que se tenga una sospecha de que se pudo filtrar la información
4) Que las contraseñas no sean fáciles de descifrar, que posean una longitud mínima, con caracteres especiales letras en mayúsculas y minúsculas y números.
5) Cuando se colocan calves comunes como por ejemplo amor, cariño, bebe, micielo o claves por este estilo, son contraseñas que son fácilmente blanco de ataques de diccionarios.

9. CONTROL DE ACCESO A SISTEMAS Y APLICACIONES.

Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones.

Controles

9.1 Restricción de acceso a información.

El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

Como implementar este control

A este punto el CEDAC ya debía haber definido concretamente los roles de sus empleados por los cual dentro de las políticas de control de acceso se debía haber establecido

1) Que usuarios y a que información pueden tener acceso
2) Que privilegios tiene el usuario con la información a la cual tiene acceso
3) Restricciones de divulgación de la información
4) Establecer controles de acceso físico y lógico para el aislamiento de datos y sistemas críticos

9.2 Procedimiento de Conexión Segura.

Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.

Como implementar este control

Para esto la entidad debe establecer mediante que formas se va a controlar la forma de conexión segura, para lo cual lo más recomendable es el uso de contraseñas con las cuales los usuarios autorizados se puedan identificar ante el sistema, cabe resaltar que estas contraseñas deben ser seguras e intransferibles y si es posible los sistemas de la empresa solo deben ser asequibles estando dentro de la red privada del CEDAC.

9.3 Sistema de Gestión de Contraseñas.

Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.

Como implementar este control

Como se explicó anteriormente el CEDAC debe de realizar capacitaciones de sensibilización en el uso adecuado de contraseñas, pero no basta solamente con esto, el sistema de identificación de las aplicaciones que la empresa maneja también debe contribuir a que se creen y cambien las contraseñas, solicitando a los usuarios cada determinado tiempo (tiempo que puede ser establecido por el CEDAC), que la contraseña sea cambiado y al ser introducida la contraseña que se va a crear que no se permita crear contraseñas cortas o con caracteres consecutivos como “12345” o “abcde” y que se incluya dentro de las contraseñas caracteres especiales, para garantizar contraseñas de calidad que no sean susceptibles a ataques de diccionario.

9.4 Uso de programas utilitarios privilegiados.

Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

Como implementar este control

Para esto el CEDAC debe de establecer unas políticas muy estrictas en el uso y descarga de programas que no estén autorizados en la entidad, para tal fin se puede recomendar el uso de usuarios con privilegios restringidos en los sistemas operativos, con el fin de que no se puedan instalar aplicaciones que no sean autorizadas por el administrador del sistema.

9.5 Control de Acceso a Códigos Fuente de Programas.

Se debe restringir el acceso a códigos fuente de programas.

Como implementar este control

Para la implementación de este control lo mejor que puede realizar el CEDAC es crear un servidor de aplicaciones con lo cual las librerías de los códigos fuentes no estarán en los equipos de los usuarios y no podrán tener acceso a los códigos fuente de los programas, en caso de que aun así se deba de tener para la ejecución correcta de una aplicación algunas carpetas en los equipos de los usuarios, se debe informar que es totalmente prohibido aun el acceso a estas carpetas y más aún modificación de su contenido y que evadir esta política de seguridad podría llevar a la aplicación del código disciplinario.

10. CRIPTOGRAFÍA

10.1. Controles Criptográficos.

Objetivo. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.

Controles

10.1.1. Política sobre el uso de controles Criptográficos.

Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.

Como implementar este control

El CEDAC puede implementar por ejemplo el uso de PKI infraestructura de clave pública para el cifrado de información confidencial o solicitar a entidades certificadores tockens, esto garantizaría integridad, confidencialidad, no repudio y autenticación.

Para los dispositivos removibles se puede utilizar el cifrado de los datos como por ejemplo la utilización de Bitlocker, el cual viene integrado con algunas versiones del sistema operativo Windows o algún otro software que la empresa considere, para mitigar el riesgo de que la información pueda ser robada o alterado en estos dispositivos.

10.1.2. Gestión de llaves.

Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.

Como implementar este control

Cuando se usan claves criptográficas se debe de establecer políticas sobre el uso y generación de estas claves para esto se puede considerar los siguiente

1) Que las claves en lo posible sean generadas por entidades certificadores
2) Si no se realiza a través de entidades certificadoras se debe garantizar que los programas con los que se crean las claves sean confiables
3) Distribuir las claves públicas a los usuarios que lo requieran para poder leer la información que reciben
4) Establecer políticas para el tratamiento de las claves privadas que se vean comprometidas
5) Realizar copias de seguridad de las claves

11. SEGURIDAD FÍSICA Y DEL ENTORNO.

11.1. Áreas Seguras.

Objetivo. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

Controles

11.1.1. Perímetro de Seguridad Física.

Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.

Como implementar este control

Para esto el CEDAC debe definir cuáles son las áreas dentro de la entidad en la que se maneja información sensible y critica para ella, como por ejemplo el área de servidores y redes la empresa debe considerar las siguientes recomendaciones

1) Crear límites físicos que impidan el acceso a estas áreas, como muros, puertas y señalizar muy bien mediante letreros de acceso restringido a personal no autorizado

11.1.2. Controles Físicos de entrada.

Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.

Como implementar este control

Para las áreas en donde se han colocado puertas para restringir su acceso se debe tomar en cuenta los siguientes controles

1) En los cuartos como por ejemplo el cuarto de servidores, la empresa debe definir qué personal tendrá llaves de acceso a este área y por que
2) El personal que posea llaves de acceso a estas áreas se debe de asegurar que una vez salga de ellas están queden cerradas y con llave
3) Mantener siempre una copia de seguridad de las llaves en caja fuerte y en caso de extravió de las mismas considerar inmediatamente el cambio de las guardas.
4) Mantener un registro de quien entra y sale del área restringida con la hora y la fecha

11.1.3. Seguridad de oficinas, salones e instalaciones.

Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones

Como implementar este control

Las instalaciones del CEDAC deben de contener avisos en donde indique que el acceso al público está restringido y solo se permite el acceso a personal autorizado, debe de contar con vigilancia las 24 horas para tener control del acceso de visitantes hacia las áreas administrativas y en lo posible mantener con llave las oficinas que así lo requieran.

11.1.4. Protección contra amenazas externas y ambientales.

Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

Como implementar este control

Para la implementación de este control el CEDAC puede contratar asesoría externa para capacitar a sus empleados en cómo actuar frente a desastres ya sea naturales como incendios, terremotos o inundaciones o causados por el hombre como por ejemplo disturbios públicos.

11.1.5. Trabajo en áreas seguras.

Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.

Como implementar este control

El CEDAC en este momento cuenta con dos áreas seguras que son el área de servidores y redes y el área de la planta eléctrica con las cuales se deben de tomar las siguientes consideraciones:

1) Todo el personal debe conocer cuáles son estas áreas y tener claro que ingresar a ellas es totalmente prohibido, sin embargo dichas áreas siempre deberán estar cerradas con llave
2) Si se necesita realizar un trabajo en estas áreas como por ejemplo limpieza o instalación de algún equipo, dicho trabajo deberá ser supervisado por el empleado responsable de estas áreas
3) Siempre deberán estar cerradas y con llave para impedir el ingreso a personal no autorizado
4) No se permitirá la toma de fotos, videos u otro equipo de grabación en estas áreas

11.1.6. Áreas de despacho y carga.

Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

Como implementar este control

Para el CEDAC no existen áreas de despacho y carga, pero si están las áreas de sala de espera de los clientes que están realizando su revisión tecnicomecanica y las áreas de post-revisión que es donde los clientes recogen sus vehículos.

Se debe garantizar que estas áreas siempre estén separadas de las áreas de oficinas y demás instalaciones en donde se encuentren activos críticos de la entidad, en el caso de

que se deba tener un cubículo dentro de unas de estas áreas como es el caso del cubículo de pago y entrega de resultados, estos deben tener unas barreras físicas que garanticen que solo el personal autorizado pueda ingresar a ellos.

11.2. Equipos.

Objetivo. Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

Controles

11.2.1. Ubicación y protección de los equipos.

Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.

Como implementar este control

Todos los equipos del CEDAC deben contar con una protección primero que todo física, que se refiere a que deben estar ubicados en una oficina o cubículo que impida que sean accedidos por personal no autorizado y también deberán contar con una cobertura como forros que impidan que los protejan agentes medioambientales como tierra, polvo o incluso goteras que puedan llegar a formarse durante una noche lluviosa y donde no había ningún personal que pudiera darse cuenta de esto.

11.2.2. Servicios Públicos de soporte.

Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.

Como implementar este control

El CEDAC cuenta con una planta eléctrica, la cual suministra energía en caso de que el suministro de la misma sea interrumpido por parte de la empresa de servicio público, sin embargo esto no es suficiente ya que mientras la planta eléctrica inicia su marcha, puede transcurrir un lapso de unos 30 segundos por lo cual los equipos se apagarían abruptamente, para impedir estos la empresa puede instalar unas UPS en la oficinas a las cuales se puedan conectar los equipos y estas se encargaran de impedir que los equipos se apaguen mientras la planta eléctrica inicia su función.

11.2.3. Seguridad del cableado.

El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.

Como implementar este control

En la medida de lo posible todo el cableado de energía eléctrica y telecomunicaciones que entran a la empresa debería hacerlo de forma subterránea, pero no ser así debe contar con la protección adecuada para impedir que sean dañados o incluso interceptados.

Los cables de energía eléctrica y los cables de comunicaciones deben de estar separados para impedir interferencias y si es necesario deben poseer un blindaje electromagnético especial para protegerlos.

11.2.4. Mantenimiento de equipos.

Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

Como implementar este control

El CEDAC puede delegar esta función a la persona encargada de los sistemas en la empresa, pero en caso de que esta persona no sea competente para la realización de los mantenimientos de los equipos, se puede contratar un personal que se encargue de este mantenimiento cada determinado periodo de tiempo (el cual deberá determinar la empresa), pero este mantenimiento debe ser realizado bajo la total supervisión de la persona encargada de los sistemas de la entidad.

11.2.5. Retiro de Activos.

Los equipos, información o software no se deben retirar de su sitio sin autorización previa.

Como implementar este control

Los activos de la entidad no se podrán retirar de la misma sin una previa autorización, sin embargo en caso de ser necesario se debe tener en cuenta las siguientes consideraciones

1) Determinar que empleado puede autorizar el retiro de un activo y bajo qué condiciones
2) Establecer hacia donde ira el activo y para que se retira de la entidad
3) Realizar un inventario completo del activo y llevar un chequeo de la fecha de salida y posible fecha de devolución con la firma de la persona que lo retira
4) Si el equipo es retirado para alguna reparación, pero el mismo lleva información crítica de la entidad se debe de establecer una cláusula de confidencialidad y no

divulgación de la información contenida en el equipo dejando claramente establecidas los delitos legales que se pueden cometer si esto sucede.

11.2.6. Seguridad de equipos y activos fuera del predio.

Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.

Como implementar este control

En el CEDAC es totalmente prohibido trabajar con equipos u activos de la organización fuera de la misma, sin embargo si se llegara a hacer netamente necesario esto se debería de tener en cuenta lo siguiente:

1) Los equipos no se pueden dejar sin ningún tipo de vigilancia por parte de la persona responsable de su uso fuera de la empresa
2) Se deben seguir todas las indicaciones del fabricante para su correcto uso fuera de las instalaciones, para evitar que este sufra algún daño
3) Instalar algún tipo de programa para monitoreo remoto y que la persona responsable de los sistemas de la empresa pueda acceder al equipo en cualquier momento y evaluar lo que en él se está realizando.

11.2.7. Disposición segura o reutilización de equipos.

Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o reúso.

Como implementar este control

Cuando un equipo es retirado por algún daño por ejemplo un daño en la Board o tarjeta madre del equipo, las unidades de almacenamiento deben ser retiradas y examinadas por la persona encargada de los sistemas de la empresa con el fin de que se extraiga de forma segura la información que se necesite y borrar de forma definitiva la unidad de almacenamiento antes de mandar a reparar el equipo, ya que al momento de enviarse a reparación se puede comprometer la información allí almacenada.

11.2.8. Equipos sin supervisión de los usuarios.

Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.

Como implementar este control

Cuando un empleado se ausente de su puesto de trabajo, debe siempre cerrar la sesión de su equipo o si no puede cerrarla ya que está ejecutando algún archivo o aplicación en el mismo debe dejar el equipo bloqueado, por ejemplo con un protector de pantalla protegido con una contraseña, para impedir que personal no autorizado pueda acceder al equipo cuando él no este, para todo esto el CEDAC debe de realizar campañas de sensibilización y constante monitoreo de los puestos de trabajo de los empleados

11.2.9. Política de escritorio limpio y pantalla limpia.

Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.

Como implementar este control

Cuando en un puesto de trabajo se maneje información importante que se encuentra en medio fisco como papel, esta jamás se debe dejar sobre los escritorios en donde sea susceptible a hurto o a que sea fotografiado con algún aparato electrónico o si se maneja un dispositivo removible nunca deben dejarse sin vigilancia sobre los escritorios, estos deben ser guardados en gabinetes o cajas fuertes con adecuada seguridad.

Si se trata de equipos como se explicó en el control inmediatamente anterior, estos deben ser bloqueados y protegidos ya sea por contraseña o algún otro medio biométrico o criptográfico.

12. SEGURIDAD DE LAS OPERACIONES.

12.1. Procedimientos operacionales y responsabilidades

Objetivo. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

Controles

12.1.1. Procedimientos de operación documentadas.

Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.

Como implementar este control

Todos los procedimientos operacionales de ser documentados como por ejemplo el procedimiento de encendido y apagado de los equipos o los procedimientos de realización de las copias de seguridad, Estos procedimientos deben estar disponibles en los sitios de trabajo para los usuarios que lo requieran.

Estos procedimientos deben estar claramente detallado paso a paso y servirán de apoyo para las personas que trabajan en esta área.

12.1.2. Gestión de Cambios.

Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

Como implementar este control

Cada vez que un burro un cambio en los procedimientos estos deben ser documentados y llevar un registro de qué cambios se hizo e inmediatamente actualizar los procedimientos con el fin de que no se cometan errores por falta de actualización de los mismos, estas muchas veces son las fallas de seguridad más comunes que se cometen

12.1.3. Gestión de Capacidad.

Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.

Como implementar este control

Se deben estar verificando constantemente que los recursos que se utilizan para llevar a cabo los procesos en el CEDAC sean estén acordes con las necesidades del servicio, si se establece que se debe mejorar un recurso, ya que para las necesidades del negocio, El recurso que se está utilizando actualmente ya no es suficiente Se debe presentar un proyecto a la alta gerencia en donde se especifique el nuevo recurso que necesita instalarse o mejorarse, una vez instalado este recurso se debe actualizar los procedimiento para impedir que se comentan errores de seguridad, ya que Ya que uno de los errores más comunes que se cometen es el no actualizar los procedimientos.

12.2. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS.

Objetivo. Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

12.2.1. Controles contra códigos maliciosos.

Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

Como implementar este control

Para poder implementar este control la empresa debe incrementar el uso de un software antivirus, con el cual se mitiguen la infección de los equipos por causas de virus o algún otro código malicioso, sin embargo se deben de crear conciencia entre los empleados, para no descargar ni tratar de instalar programas no autorizados que puedan tener oculto algún código malicioso. El software antivirus que se utilice debe estar correctamente el Licenciado y es preferible que también posea escudos de red.

12.3. COPIAS DE RESPALDO.

Objetivo. Proteger contra la pérdida de datos.

Controles

12.3.1. Copias de respaldo de la información.

Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

Como implementar este control

Para esto se debe establecer cada cuánto tiempo se deben realizar las copias de seguridad, En el CEDAC es necesario realizar las copias de seguridad de las revisiones técnico mecánicas Diariamente Ya que en así lo establecen la norma NTC 5385. Cada vez que se realiza una copia de seguridad, Esta se debe almacenar en un disco duro que se encuentra alojado en el servidor de datos Y a su vez se debe almacenar en un disco duro extraíble el cual se debe almacenado fuera del cuarto de servidores en una caja fuerte.

Estas copias de seguridad siete deben verificar cada determinado período de tiempo que puede ser por lo menos cada mes.

12.4. REGISTRO Y SEGUIMIENTO.

Objetivo. Registrar eventos y generar evidencia.

Controles

12.4.1. Registro de eventos.

Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.

Como implementar este control

Los registros de eventos deben incluir por ejemplo:

1) Identificación de usuarios
2) Actividades del sistema
3) Fechas horas y detalles de los eventos por ejemplo entrada y salida
4) Identidad del dispositivo ubicación si es posible e identificados del sistema
5) Cambios en la configuración del sistema
6) Uso de utilidades y aplicaciones
7) Activación y desactivación de los sistemas de protección tales como antivirus

Estos registros estables en bases para el sistema de seguimiento automatizados y pueden estar en capacidad de generar informes consolidados.

12.4.2. Protección de la información de registro.

Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.

Como implementar este control

Los registros del sistema deben estar protegidos contra alteraciones y acceso no autorizado, Incluso los usuarios con privilegios como administradores deben tener restringido la capacidad de alterar o borrar los registros de sus propias actividades

12.4.3. Registros del administrador y del operador.

Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.

Como implementar este control

Los usuarios privilegiados podían estar en la capacidad de manipularlo registros por esto es necesario proteger y revisar los registros Para mantener la rendición de cuentas de los usuarios privilegiados.

12.4.4. Sincronización de relojes.

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.

Como implementar este control

Dentro de la configuración de los sistemas operativos, se puede establecer que todo lo relojes se sincronicen con un servidor en particular, Este servidor por ejemplo puede ser el del NIST National Institute of Standards and Technology, El cual lleva la hora mundial y sólo se deberán escoger La zona horaria donde nos encontramos Que para Colombia que es la UTC que -5:00 horas.

12.5. CONTROL DE SOFTWARE OPERACIONAL.

Objetivo. Asegurarse de la integridad de los sistemas operacionales.

Controles

12.5.1. Instalación de software en sistemas operativos.

Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.

Como implementar este control

Una de las mejores formas de implementar este control Es crear usuarios un privilegio restringidos, Los cuales no poseían los permisos para poder instalar software en los sistemas operativos y que sólo con permisos que el usuario administrador se pueden instalar cualquier tipo de software. Con esto se garantiza que sólo los administradores o el administrador del sistema sería el único que pueda instalar software en los equipos de la entidad.

12.6. GESTIÓN DE VULNERABILIDAD TÉCNICA.

Objetivo. Prevenir el aprovechamiento de las vulnerabilidades técnicas.

Controles

12.6.1. Gestión de las vulnerabilidades técnicas.

Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

Como implementar este control

Uno de los primeros pasos y muy importantes es mantener actualizados siempre el inventario de activos, El CEDAC debe definir y establecer muy bien los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica Y establecer protocolo para identificar los riesgos asociados y las acciones para tomar en caso de que se identifique una vulnerabilidad.

Si existen parche que puedan instalar en el sistema para mitigar las vulnerabilidades se puede considerar instalarlos, Sin embargo es importante probar que estos parches no produzcan efectos secundarios en los sistemas de ser así se puede considerar otro tipo de controles como por ejemplo:

1) Adicionar controles de acceso como por ejemplo, firewalls en los límites de la red
2) Incrementar el seguimiento para detectar ataques reales
3) Hacer toma de conciencia sobre la vulnerabilidad encontrada.

12.6.2. Restricciones sobre la instalación de Software.

Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.

Como implementar este control

Para cumplir con este control la empresa debe definir una política clara y estricta que debe hacer cumplir con relación al software que pueden instalar los usuarios, Para esto es mejor establece el principio que cualquier instalación del software está prohibida y sólo bajo la autorización del Administrador del sistema puede realizarse.

12.7. CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN.

Objetivo. Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.

Controles

12.7.1. Controles sobre auditorías de Sistemas de Información.

Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.

Como implementar este control

Se debe de observar lo siguiente en estas auditorías de sistema de información.

1) Los requisitos de auditoría para acceso sistema y a datos se deberían acordar con la dirección apropiada
2) El alcance y las pruebas técnicas de auditoría se deben acordar y controlar
3) Realizar todo un seguimiento a los accesos y registrarlos

13. SEGURIDAD DE LAS COMUNICACIONES.

13.1. GESTIÓN DE SEGURIDAD DE REDES.

Objetivo. Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

Controles

13.1.1. Controles de redes.

Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.

Como implementar este control

El CEDAC debe implementar todas unas políticas para asegurar la seguridad de la información en la red de la empresa, todos los equipos en la red de la entidad se deben de autenticar y establecer las responsabilidades sobre el adecuado funcionamiento de la red, incluso se deben establecer controles para mantener la disponibilidad de los servicios de red y computadores que se conecten a esta.

Cuando se disponen de redes WIFI estas deben de poseer una clave segura para su conexión y que solamente sea conocida por el administrador de la red, los recursos compartidos dentro de la red de la entidad deben estar protegidos por ejemplo mediante conexión con usuario y contraseña y dichos recursos deben estar supervisados por el administrador de la red.

13.1.2. Seguridad de los servicios de red.

Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

Como implementar este control

Se deben establecer con el proveedor de servicios de red una forma segura para la prestación de los servicios y hacer seguimiento al mismo y acordar con ellos el derecho a auditorias

Unas características de seguridad en la redes pueden ser:

1) Tecnologías aplicadas tales como autenticación, criptografía y controles de conexión a red
2) Los procedimientos para restringir el acceso a los servicios y aplicaciones de red cuando se requiera.

13.1.3. Separación en las redes.

Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.

Como implementar este control

La red LAN del CEDAC es una red pequeña, la cual podría separarse solo con la aplicación de dos dominios, uno que pertenezca al área operativa y el otro dominio que sea para el área administrativa, algo muy importante que cabe resaltar es que en ningún momento se debe de permitir el acceso a las redes de la entidad a los clientes de la empresa, para esto es preferible contratar un servicio de internet aparte de la red privada de la empresa y de esta forma mitigar el riesgo de que usuarios puedan efectuar ataques dentro de la red LAN de la entidad.

13.2. Transferencia de información.

Objetivo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

Controles

13.2.1. Políticas y procedimientos de transferencia de información.

Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.

Como implementar este control

Para la transferencia segura de información el CEDAC debe considerar la implementación de controles que ayuden a proteger la información transferida de copiado, modificación o borrado, mediante por ejemplo el uso de controles criptográficos con los cuales la información se puede codificar y de esta forma asegurarse de que solo el destinatario deseado pueda descifrarla y leer o modificar la información que se envió.

Capacitar al personal para que tomen conciencia de la gravedad de revelar información confidencial de la entidad y no mantener conversaciones confidenciales en lugares públicos.

13.2.2. Acuerdos sobre transferencia de información.

Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.

Como implementar este control

La transferencia de información con partes externas a la entidad cuando asi se requiera debe incluir:

1) La dirección debe ser responsable por el control del envió, despacho y recibo de la información
2) Procedimiento para poder realizar un a trazabilidad a la información
3) Cuando la información se envía en medio magnético esta debe ser correctamente empacada y protegida de cualquier factor ambiental
4) Usar siempre correos certificados para garantizar que la información es recibida solo en el lugar y por el usuario al cual se le envía.
5) Mantener toda una cadena de custodia de la información cuando esta está en transito

13.2.3. Mensajes electrónicos.

Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.

Como implementar este control

El CEDAC solo maneja un correo electrónico y por lo cual el mismo solo puede ser accedido por personal autorizado y los mismos tendrán la responsabilidad de revisar los mensajes tanto que llegan al correo como los mensajes que se envían, para impedir que se pierda información importante o que se envié información confidencial a través de este

correo. Pero en este control no solo se debe de considerar el correo electrónico sino también las redes sociales como Facebook, twitter o Instagram, en las cuales se debe de tener estricto monitoreo para verificar la información que se está compartiendo.

13.2.4. Acuerdos de confidencialidad o de no divulgación.

Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

Como implementar este control

En los acuerdos de confidencialidad ele CEDAC no solo los debe establecer con sus empleados y contratistas según el tipo de información que manejen, sino también con los proveedores teniendo en cuenta el tipo de contratación que con este se tenga

1) Se deben manejar en los acuerdos de confidencialidad, términos ejecutables legalmente
2) Cuanto será la duración de un acuerdo y si es considerable este puede ser de for indefinida
3) Que responsabilidades legales tienen los firmantes de los acuerdos
4) Si hay información que debe ser devuelta una vez terminado el acuerdo, se debe de establecer un tiempo para dicha devolución y dejar claro que sanciones legales pueden ponerse en su contra en caso de que la información no sea devuelta.
5) Estos acuerdos se deben de revisar de forma periódica y cuando se considere pertinente realizar algún cambio se deben incluir y notificar al empleado, contratista o proveedor.

15. RELACIONES CON LOS PROVEEDORES.

15.1. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES.

Objetivo. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

Controles

15.1.1. Política de seguridad de la información para las relaciones con proveedores.

Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.

Como implementar este control

El CEDAC debe de implementar unas políticas para mantener seguros los activos de la empresa ante algunos proveedores que puedan tener acceso a ellos, como por ejemplo los proveedores de software y de mantenimiento de equipos, con ellos se debe de firmar unos acuerdos de confidencialidad y no divulgación de la información a la que puedan tener acceso también definir:

1) Quien tendrá la responsabilidad de realizar seguimiento y supervisión a los proveedores
2) Los controles que tendrá la entidad con los proveedores deberán ser informados a los mismos para que tengan claro conocimiento de lo que deben cumplir.
3) Ser muy claro con los proveedores del alcance y tiempo de la responsabilidad de confidencialidad y no divulgación nombrando la terminología legal que se requiera.
4) Llevar un registro de las actividades de los proveedores con fecha hora y tipo de actividad como evidencia para alguna auditoria.

15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores.

Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.

Como implementar este control

Como ya se mencionó en el control inmediatamente anterior, el CEDAC debe documentar los controles que se van a establecer para asegurar la información que se requiera suministrar a los proveedores y a su vez se debe comunicar a los proveedores estos controles con el fin de que no existan malos entendidos entre ninguna de las partes involucradas dentro de stos acuerdos se tiene que dejar claro:

1) Tipo de información que se va a suministrar al proveedor y de que forma la misma será suministrada
2) Dejar claro todos los requisitos legales, como la protección de los datos, la propiedad intelectual, derechos de autor y de que forma estos se hará cumplir
3) Dejar claro con el proveedor que estará siendo supervisado, evaluando su desempeño y asegurando que los controles de seguridad se cumpla.
4) Se deben establecer entre ambas partes procesos de solución de defectos y conflictos
5) Todos los acuerdos deben estar correctamente firmados y socializados entre ambas partes antes de iniciar con los procesos.

15.1.3. Cadena de suministro de tecnología de información y comunicación.

Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

Como implementar este control

Este control para el CEDAC está muy relacionado con los proveedores de software de revisión y software contable con los cuales se deben establecer controles especiales ya que se deben suministrar servicios de comunicación especiales como lo son las conexiones remotas para poder prestar soporte en caso de que se requiera, para esto se debe acordar con los proveedores incluso hasta en que horarios se puede suministrar este soporte y que el mismo estará constantemente monitoreado y que es totalmente prohibido copiar información de los equipos a los que se les está prestando soporte y que la misma es de carácter confidencial y su divulgación está totalmente prohibida, es necesario que los proveedores acepten las políticas de seguridad de la empresa de lo contrario no se podría establecer un acuerdo con los mismos.

15.2. GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES.

Objetivo. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

Controles

15.2.1. Seguimiento y revisión de los servicios de los proveedores.

Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

Como implementar este control

El CEDAC mediante los seguimientos que realiza a los proveedores, debe de evaluar cuál es el desempeño de los mismos y verificar no solo que esté cumpliendo con el trabajo para el cual se contrató sino que también cumpla con todas las políticas de seguridad que se acordaron, se pueden solicitar también a los proveedores un informe de las actividades realizadas y de esta forma verificar si se lograron los objetivos que se contrataron.

El encargado de supervisar el trabajo de los proveedores es una ficha clave en la evaluación del desempeño de los mismos y los registros que se lleven también se podrán usar como soporte de dicha revisión de los servicios prestados.

15.2.2. Gestión de cambios a los servicios de los proveedores.

Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.

Como implementar este control

Se deben estar verificando constantemente, las políticas de seguridad de la información acordada con los proveedores y de ser necesario modificarlas para una mejora, porque se han identificado nuevos riesgos o porque el servicio que ahora presta el proveedor así lo requiere, estas nuevas políticas se deben de documentar y comunicar a los proveedores para que sean aceptadas y no existan conflictos a futuro por falta de comunicación entre las partes.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

16.1. GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN.

Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.

Controles

16.1.1. Responsabilidades y procedimientos.

Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Como implementar este control

El CEDAC debe documentar muy bien los procedimientos de respuestas a incidentes en la seguridad de la información y las responsabilidades de gestión para comunicar estos procedimientos.

1) Como se comunica un evento de incidente de seguridad de la información
2) Como se registrara este incidente
3) Procedimiento para el manejo de la evidencia forense en el equipo que se llevó a cabo el incidente.

Los procedimientos llevaran

1) El personal competente que manejara todo lo relacionado con el incidente
2) Que tratamiento se le dará al incidente
3) De qué forma se le dará superación al incidente y si hay que iniciar algu n método de recuperación

Los reportes pueden incluir

1) Todos los procedimientos que se siguieron para este incidente de seguridad informática
2) El lugar donde quedo registrado todo lo sucedido incluyendo la evidencia forense que se haya conseguido
3) Si se lleva a cabo un proceso formal disciplinario establecido para aplicar a los empleados que se demuestre que estuvieron involucrados en el incidente.
4) Proceso para comunicación para notificar los resultados a las personas que informaron el incidente de seguridad de la información

16.1.2. Informe de eventos de seguridad de la información.

Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible

Como implementar este control

El CEDAC debe de comunicar a los empleados y contratistas cuales pueden ser eventos de seguridad de la información, los cuales pueden ser reportados para su correcto tratamiento y tomar conciencia de la importancia y el impacto positivo que puede traer a la empresa reportar estos eventos, un incidente de seguridad poder ser:

1) Un control de seguridad débil
2) Alteración, modificación o barrado de la información confidencial de la empresa
3) Violación de restricciones de acceso físico o lógicos
4) Mal funcionamiento de un sistema operativo, aplicación o algún hardware

16.1.3. Informe de debilidades de seguridad de la información.

Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

Como implementar este control

Este control más que crear un procedimiento y documentarlo, lo que se debe de crear es conciencia entre los empleados y contratistas para que informen al responsable del sistema de la debilidad que se ha encontrado y que podría terminar en un incidente de seguridad de la información, no deben internar aprovechar las debilidades del sistema para probarlo ya que pueden incurrir en una violación de las políticas de seguridad y se podría iniar en su contra un proceso disciplinario.

16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos.

Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.

Como implementar este control

Se debe de crear una escala de valoración de los eventos e incidentes de seguridad de la información y de esta forma poder catalogar si lo que ha ocurrido se clásica como un incidente de seguridad y reportarlo como tal, esto quiere decir que si no clásica como incidente no se deba reportar aun así se debe realizar un reporte documentando lo sucedido aunque este no sea clasificado como incidente.

16.1.5. Respuesta a incidentes de seguridad de la información.

Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

Como implementar este control

Para que las personas designadas para responder a los incidentes puedan dar una adecuada respuesta a los mismos pueden seguir los siguientes pasos

1) Poner en práctica técnicas de informática forense para la recolección de evidencia lo más pronto posible
2) Comunicar la existencia de un incidente de seguridad de la información solo al personal que así lo requiera
3) Porque ocurrió el incidente, en donde estuvo la debilidad del sistema
4) Cuando el incidente ya se le allá dado el adecuado tratamiento se debe de cerrar y hacer un registro del mismo
5) Buscar el origen del incidente para fortalecer la debilidad que lo origino.

16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información.

El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.

Como implementar este control

Toda la información que se recolecto tras resolver un incidente de seguridad, se debe de utilizar para identificar incidentes recurrentes y también para fortalecer las debilidades que el sistema pueda tener y mitigar aún más el riesgo de que un incidente se vuelva a presentar.

16.1.7. Recolección de evidencia.

La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

Como implementar este control

El CEDAC debe de establecer procedimientos para el tratamiento de evidencia y más aún cuando dicha evidencia será utilizada para propósitos legales cuando se trata de tratamiento de evidencia se pueden apoyar en la técnicas de informática forense las cuales pueden ser:

1) Cadena de custodia de la evidencia
2) Seguridad que se le dará a la evidencia
3) Responsabilidad de la persona encargada de la evidencia
4) El personal que maneja esta evidencia debe ser idóneo para esto

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.

17.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.

Controles

17.1.1. Planificación de la continuidad de la seguridad de la información.

La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.

Como implementar este control

Como ya se ha mencionado con anterioridad dentro de la seguridad de la información deben de estar contempladas las copias de seguridad y respaldo de la información de la empresa, las cuales debe estar disponibles ante una eventualidad o desastre para garantizar que la empresa pueda seguir operando.

17.1.2. Implementación de la continuidad de la seguridad de la información.

La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

Como implementar este control

Dentro de los procedimientos establecidos por el CEDAC para la continuidad del negocio se deben de incluir la continuidad de la seguridad de la información, más en una empresa como esta en donde es indispensable la base de datos de las revisiones para poder llevar a cabo se razón social, de tal forma que dentro de los procesos de continuidad del negocio ante desastres o alguna otra eventualidad se deben tener claros los procesos de recuperación y restauración de la información de las copias de seguridad e incluir equipos de respaldo para este fin.

17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

Como implementar este control

Una de las mejores formas de implementar este control es poner en marcha los procedimientos de continuidad del negocio como si fuese un simulacro y de esta forma determinar si los procedimientos establecidos son eficientes y pueden garantizar la continuidad del negocio, todo esto debe ser documentado y si existe alguna mejora se debe de registrar y modificar en los procedimientos los cuales se socializaran nuevamente entre las personas que tengan esta responsabilidad.

17.2. REDUNDANCIA

Objetivo. Asegurarse de la disponibilidad de instalaciones de procesamiento de información.

Control

17.2.1. Disponibilidad de instalaciones de procesamiento de información.

Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Como implementar este control

En el CEDAC se cuentan con dos servidores los cuales poseen la información más crítica de la empresa como lo es la base de datos de las revisiones, la base de datos contable y el sistema de gestión de calidad, estos servidores posee discos duros espejo, es decir que la información que se está grabando en un disco simultáneamente se está grabando en otro con lo cual se cumple con la redundancia de datos ya que si se daña un disco duro toda la información quedara en el otro disco redundante sin embargo esto debe ser probado y verificar que la información si es disponible y confiable al momento que se necesite y registrar todos estos procedimientos.

18. CUMPLIMIENTO.

18.1. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES.

Objetivo. Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

Controles

18.1.1. Identificación de los requisitos de legislación y contractuales aplicables.

Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes, y el enfoque de la organización para cada sistema de información y para la organización.

Como implementar este control

El CEDAC debe verificar todos los requisitos legales vigentes en la legislación colombiana que le sean aplicables a su negocio y documentar absolutamente todos los controles y las responsabilidades dentro de todo este proceso de seguridad de la información.

18.1.2. Derechos de Propiedad Intelectual.

Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.

Como implementar este control

El CEDAC debe de tener registrado absolutamente todos los software que se utilizan para llevar a cabo las actividades de la empresa y especificar para cada uno su respectiva licencia o permisos del desarrollador del software para su uso, con el fin de asegurar que no se usa software pirata y no se están violando los derechos de autor.

18.1.3. Protección de registros.

Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.

Como implementar este control

La empresa debe de establecer unos protocolos adecuados para la protección de los registros, cuando son medios físicos se debe considerar la posibilidad del deterior por factores medio ambientales como calor, humedad o incluso plagas, por lo cual se deben de tomar las medidas necesarios para la correcta conservación de todos los registros

Cuando se decide almacenar en medios electrónicos se debe garantizar que la información contenida se puede recuperar facialmente y si es posible almacenarlas en dos medios redundantes los cuales no se almacenen en el mismo sitio, para evitar que si ocurre un desastre natural no afecten ambas copias de la información.

Se debe establecer para cada uno de los casos por cuánto tiempo se debe de tener almacenada esta información, para esto hay que revisar la normatividad y si es el caso leyes vigentes para tal fin.

18.1.4. Privacidad y protección de la información identificable personalmente.

Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.

Como implementar este control

Para esto la empresa se puede apoyar en la ley 1581 de 2012 en la cual se dictan las disposiciones generales para la protección de datos personales. Estos apoyado en un funcionario que sea el responsable de la privacidad quien deberá orientar a el gerente usuarios, empleados, contratistas y proveedores de los procedimientos que deben seguir para la protección de los datos personales y que sus datos personales con el CEDAC estarán seguros y no se divulgaran a menos de que una orden judicial así lo requiera.

18.2. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.

Controles

18.2.1. Revisión independiente de la seguridad de la información.

El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, la políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

Como implementar este control

La revisión independiente debe ser llevada a cabo por individuos que no pertenezcan al área que se está revisando con el fin de mantener una imparcialidad y verificar que todo se está cumpliendo, esta revisión debe incluir la valoración de las oportunidades de mejora y todos los resultados de esta revisión se deberán registrar y reportar a la dirección que dio inicio a la revisión.

18.2.2. Cumplimiento con las políticas y normas de seguridad.

Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.

Como implementar este control

Se deben establecer cómo se verificara que todas las políticas establecidas en el sistema de seguridad de la información se estén cumpliendo, el mayor responsable de esto será la alta gerencia para esto se puede solicitar un servicio de auditoria externa que evalué el cumplimiento y si se encuentra alguna no conformidad en el cumplimiento la gerencia deberá:

1) Identificar las causas
2) Evaluar la necesidad de acciones para lograr el cumplimiento
3) Impl4ementar acciones correctivas

18.2.3. Revisión del Cumplimiento Técnico.

Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Como implementar este control

Para la verificación del cumplimiento técnico la empresa se puede apoyar en un ingeniero de sistemas experimentado en procesos de Penetration Test y valoración de vulnerabilidades, todas estas prácticas pueden requerir de software especializado por lo que se deben llevar con mucho cuidado, las mismas se deben planificar, documentar y registrar.

ORIGINAL FIRMADO-

CEDAC CÚCUTA
REVISIÓN TECNOMECÁNICA Y DE EMISIONES CONTAMINANTES

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y CONTROLES DE LA SEGURIDAD DE LA INFORMACIÓN