FUNDACIÓN UNIVERSITARIA ANTONIO DE ARÉVALO - UNITECNAR

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Cartagena de Indias D.T. y C., Bolivar.
2020

UNITECNAR

TABLA DE CONTENIDO

2 INTRODUCCION 4

3 OBJETIVOS 4

3.1 2.1. OBJETIVO GENERAL 4

4 ALCANCE 4

5 MARCO LEGAL 4

6 MARCO CONCEPTUAL 6

7 DESARROLLO DEL PLAN 10

7.1 INTRODUCCION AL SISTEMA DE SEGURIDAD DE LA INFORMACION 10

7.1.1 SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 10

7.1.2 ESTÁNDARES DE GERENCIA DE LA INFORMACIÓN. 10

7.1.3 POR QUE LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN UNITECNAR 11

7.2 POLITICA DE SEGURIDAD DE LA INFORMACION 11

7.2.1 RESPONSABILIDAD 11

7.3 ASPECTOS ORGANIZATIVOS DE LA GESTIÓN DE ACTIVOS: INVENTARIO DE ACTIVOS DE INFORMACIÓN 12

7.3.1 DECLARACIÓN 13

7.3.2 RESPONSABILIDAD DE LOS ACTIVOS DE INFORMACIÓN. 13

7.4 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS. 13

7.5 CONTROL DE ACCESO. 14

7.6 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN. 15

7.7 PROTECCIÓN CONTRA SOFTWARE NOCIVO 15

7.8 PROTECCIÓN DURANTE LA NAVEGACION EN INTERNET. 16

7.9 SEGURIDAD DEL CORREO ELECTRÓNICO 17

8 ESTRATEGIAS 19

8.1 ESTRATEGIA 1: ACTUALIZACIÓN DEL INVENTARIO DE ACTIVOSDE INFORMACIÓN 19

8.2 ESTRATEGIA 2: IDENTIFICACIÓN Y VALORACIÓN DE RIEGOS DE SEGURIDAD DE LA INFORMACIÓN 19
8.3 ESTRATEGIA 3: ESCOGER Y FORMALIZAR LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN 19
8.3.1 ETIQUETADO Y MANEJO DE LA INFORMACIÓN 19
8.3.2 ESCRITORIO LIMPIO. 19
8.4 ELABORAR LOS INDICADORES DE SEGURIDAD DE LA INFORMACIÓN Y REALIZAR LA MEDICIÓN 21
9 ASPECTOS GENERALES 23
9.1 ESTRUCTURAORGÁNICA 23
9.2 ROLES Y RESPONSABILIDADES 24
10 DOCUMENTOS RELACIONADOS 24

1 INTRODUCCION

UNITECNAR trabaja continuamente en la mejora de la Seguridad de la Información para los procesos institucionales que busca mejorar en pro de brindarle un mayor respaldo en la custodia de los datos personales de nuestros Estudiantes, Empleados, Usuarios, Clientes y Proveedores. En este sentido y bajo el marco de la normatividad vigente que rige el sistema de seguridad de información y el Registro Nacional de Base de Datos, de acuerdo a la Ley 1266 De 2008, Ley 1273 De 2009, Decreto Número 1377 De 2013, Ley 1712 De 2014, Decreto 1008 De 2018, y bajo los parámetros establecidos en la Norma ISO 27001. Se establece el presente documento donde se definen las actividades que se realizan actualmente y las estrategias planteadas para alcanzar este propósito.

2 OBJETIVOS

2.1 2.1. OBJETIVO GENERAL

Proveer a la Institución de las directrices principales en cuanto a Seguridad de la Información desde el punto de vista institucional, considerando aspectos de seguridad lógica, física y ambiental, generando un marco para el desarrollo y aplicación de las políticas de seguridad, como herramienta para la gestión de la respuesta ante incidentes de seguridad de la información y definir los procedimientos que se requieren al efecto.

3 ALCANCE

Abarca todo el conjunto articulado de acciones para gestionar las bases de datos de información de UNITECNAR, en los aspectos de seguridad, incluyendo el diagnóstico, la actualización de la política, la elaboración del inventario de activos de información, escogiendo y formalizando los controles de seguridad de la información, elaborando y realizando medición y monitoreo de los indicadores de seguridad.

4 MARCO LEGAL

LEY 594 de 2000: Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

LEY 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

NTC-ISO/IEC 27001: Norma Técnica Colombiana que especifica los requisitos para establecer, documentar, implementar, operar, seguir, revisar y mantener un Sistema de Gestión de la Seguridad de la Información.

LEY 1266 DE 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Esta ley busca dar a conocer a las personas el derecho que tienen sobre conocer su información contenida en bases de datos y garantizarle el manejo de esta además de mantenerla actualizada. La ley es aplicable al proyecto puesto que UNITECNAR maneja información en sus bases de datos de los aspirantes estudiantes, docentes, personal administrativo y proveedores los cuales podrían acceder en cualquier momento mediante esta ley a ejercer su derecho de rectificar su información y actualizarla.

LEY 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Esta ley busca identificar los delitos informáticos y darle un valor ante la justicia para poder procesar a los individuos que infrinjan los artículos expresados en la ley. La ley es congruente con el proyecto puesto que la institución maneja distintos softwares, cuenta con un sitio web, numerosos activos informáticos y maneja información personal y financiera de personas.

DECRETO NÚMERO 1377 DE 2013: Dicta Que mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1, tiene por objeto "(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma”.

Este decreto es aplicable al proyecto ya que la institución tiene sistemas para

correcta recolección de los datos de las personas (estudiantes, docentes y administrativos), y estos pueden verificar su correcto almacenamiento y tratamiento a sus datos.

LEY 1712 DE 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Esta ley también es llamada ley de transparencia puesto que les da las facultades a las personas de poder acceder a la información pues esta se considera publica, sin dejar de lado las condiciones y procedimientos que se requieren para esto, cuando se dice condiciones se refiere a que existe información que es considerada constitucionalmente como excepción.

DECRETO 1008 DE 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Este decreto es aplicable al proyecto puesto que busca promover la seguridad para con el usuario final mediante reglamentaciones que garanticen el acceso a la información en línea de una forma ininterrumpida y actualizada.

5 MARCO CONCEPTUAL

ACTIVOS DE INFORMACIÓN: Cualquier elemento que recopile, almacene, procese o distribuya la información en la entidad y que tenga valor para la misma.

Los Activos de Información son todo aquello que UNITECNAR considera importante o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos con usuarios, contraseñas, etc.

En general es toda la información que la entidad posee dentro de un activo informático tales como servidores, Bases de Datos, Sistemas de Información, etc.

ANÁLISIS DE CAUSAS: Es una metodología que contiene un conjunto de herramientas, las cuales son usadas para la identificación de las causas por cuales ocurre una determinada situación que afecta los objetivos y metas institucionales.

AUTORIZACIÓN: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

AVISO DE PRIVACIDAD: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

DATO: Cifra, concepto e instrucción que no tiene ni un contexto definido ni correlación entre sí, siendo una representación simbólica de algo.

BASE DE DATOS: Conjunto de información digital o física, ordenada y almacenada, que es susceptible a tratamiento.

DATO PERSONAL: Información vinculada o que se pueda vincular a una o varias personas naturales determinables o no determinables y que puede ser identificada. Por ejemplo: Nombres, dirección, número telefónico, correo eléctrico, estado civil, fotografía, huella dactilar.

DATO PERSONAL PRIVADO: Es un dato personal que por su naturaleza íntima o reservada sólo interesa a su titular y para su tratamiento requiere de su autorización expresa. Por ejemplo: Nivel de escolaridad, presencias comerciales, gustos personales, entre otros.

DATO PERSONAL SEMIPRIVADO: Son aquellos datos personales que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular, sino a un grupo de personas o a la sociedad en general. En este caso, para su tratamiento se requiere la autorización expresa del titular de la información. Por ejemplo: datos de carácter financiero, datos relativos a las relaciones con las entidades de seguridad social (EPS, AFP, ARL, Cajas de Compensación), sociedades a las que pertenece entre otros.

DATO PERSONAL SENSIBLE: Es aquella información que afecta la intimidad de su titular por lo que su uso indebido puede generar su discriminación, tales como aquellas que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como la información relativa a la salud, a la vida sexual y los datos biométricos.

Esta información No puede ser objeto de tratamiento a menos que sea requerida para salvaguardar un interés vital del titular o éste se encuentre incapacitado y su obtención haya sido autorizada expresamente.

DATO PERSONAL PÚBLICO: Es aquel tipo de dato personal que las normas y la Constitución han determinado expresamente como públicos y, para cuya recolección y tratamiento, no es necesaria la autorización del titular de la información. Por ejemplo: estado civil de las personas, datos contenidos del RUNT, datos contenidos en sentencias judiciales ejecutoriadas, entre otros.

ENCARGADO DEL TRATAMIENTO: Es aquella persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

RESPONSABLE DEL TRATAMIENTO: Es aquella persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

TITULAR: es aquella persona natural, dueña del dato personal y que debe autorizar su tratamiento. En el caso de los menores de edad, sus representantes legales tendrán la facultad de autorizar o no el tratamiento de sus datos personales.

TRATAMIENTO: Es cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

TRANSFERENCIA: La transferencia de datos tiene lugar cuando el responsable o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

TRANSMISIÓN: tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

INFORMACIÓN: Conjunto de datos estructurados y procesados con valor agregado que se transforman en conocimiento útil para tener ventaja competitiva. Ésta, para efectos de utilidad en UNITECNAR, debe ser relevante, completa, precisa, actual, veraz.

NECESIDADES DE INFORMACIÓN: Consiste en la insuficiencia de conocimiento o información de las partes interesadas acerca de un aspecto específico y que se requiere como insumo para ser transformada por éstas o simplemente ser consultada.

PARTES INTERESADAS: Son las personas y las organizaciones quienes pueden ser afectadas, afectan o perciben que ellos mismos pueden ser afectados por una decisión o actividad de UNITECNAR.

PRINCIPIO DE CONFIDENCIALIDAD: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

PRINCIPIO DE LEGALIDAD: El Tratamiento de datos personales es una actividad reglada que debe sujetarse a lo establecido en la ley y en las demás disposiciones que la desarrollen.

PRINCIPIO DE CONFIDENCIALIDAD: Se trata de la cualidad que debe poseer un documento o archivo para que esté solo se entienda de la manera comprensible o sea leído por la persona o sistema que esté autorizado. De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y solo si puede ser comprendido por la persona o entidad a quien va dirigido o esté autorizado.

PRINCIPIO DE INTEGRIDAD: La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original. Aplicado a las bases de datos sería la correspondencia entre los datos y los hechos que refleja. En el caso del envío de la información y su no modificación durante su viaje a través de una red.

PRINCIPIO DE DISPONIBILIDAD: Se trata de la capacidad de un servicio de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran. También se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

PRINCIPIO DE TRANSPARENCIA: En el Tratamiento debe garantizarse el

derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

REGISTRO NACIONAL DE BASES DE DATOS: es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, la integridad y la disponibilidad de la información

TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: Se definen como el conjunto de herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes.

VARIACIONES NO ESPERADAS: Es el cambio de los resultados esperados o la tendencia en la información detectado en el análisis periódico.

6 DESARROLLO DE LA POLÍTICA

6.1 INTRODUCCION AL SISTEMA DE SEGURIDAD DE LA INFORMACION

6.1.1 SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

En UNITECNAR nos comprometemos a direccionar nuestra gestión de manera integral, asegurando el Sistema de Gestión de Seguridad de la Información. Para este propósito la entidad implementa el Sistema de Gestión de Seguridad de la Información (SGSI) que busca la confidencialidad, integridad y disponibilidad de la información que se maneja dentro de la Institución a través de la norma ISO 27001 y demás normas aplicables.

6.1.2 ESTÁNDARES DE GERENCIA DE LA INFORMACIÓN.

La sección de los estándares de la gerencia de la información pretende señalar los elementos sustanciales de la organización para el diseño y puesta en marcha de un proceso coherente de gerencia de la información y de los recursos utilizados para su adecuado desarrollo. Implica el facilitar las decisiones de los trabajadores de la organización (en todo nivel), basados en la integración de la información originada por los procesos. La gerencia de la información debe garantizar la estructura y coherencia de la información para generar habilidades de respuesta a los

requerimientos de los estudiantes, clientes, usuarios, proveedores y trabajadores.

6.1.3 POR QUÉ LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN UNITECNAR

La información en términos normativos es un bien que debe ser protegido y preservado. En tal sentido UNITECNAR crea mecanismos que garanticen estos preceptos teniendo siempre presente el respeto por los usuarios y demás personas interesadas.

6.2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

UNITECNAR, considera la información de vital importancia para su normal desempeño. Por este motivo, establece que los activos de información son críticos y deben ser protegidos de todo tipo de amenazas, deliberadas o accidentales para garantizar la continuidad de la prestación de los servicios académicos.

En este sentido la institución velara por proteger y asegurar la integridad, disponibilidad y confidencialidad de los activos de información durante su ciclo de vida independiente de los medios de soporte y tratamiento, realizando la gestión de los riesgos de seguridad de la información por medio de la implementación, monitoreo y mejora continua de los controles y medidas que minimicen dichos eventos, fortaleciendo la cultura de seguridad en los empleados en el marco de la normatividad legal vigente.

6.2.1 RESPONSABILIDAD

Los Integrantes de la Alta Dirección, son responsables de la implementación de las Políticas de Seguridad de la Información. Incluyendo la gestión de los Activos de Información.
Las Políticas de Seguridad de la Información son de Carácter Obligatorio para todo el personal de la Entidad, cualquiera sea su situación laboral o el área en la cual se encuentre laborando. Estas Políticas también aplican a los terceros que tengan alguna relación con la entidad.

6.2.1.1 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

La División de Tecnologías y Sistemas de Información cumplirá funciones relativas a la seguridad de los sistemas de información de UNITECNAR, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

6.2.1.2 USUARIOS DE LA SEGURIDAD DE LA INFORMACIÓN

Son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

Son responsables los líderes de proceso de mantener actualizado los activos de información a su cargo.

6.2.1.3 COMITÉ TÉCNICO DE SISTEMAS DE INFORMACIÓN

La Vicerrectoría De Calidad Institucional, la Vicerrectoría de Planeación y Gestión Administrativa, Secretaría General y Jurídica y la División de Tecnologías y Sistemas de Información son responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por estas Políticas y por las Normas, Procedimientos y prácticas que de ella surjan.

6.2.1.4 SANCIONES PREVISTAS POR INCUMPLIMIENTO

El incumplimiento de las Políticas podrá dar lugar a un proceso disciplinario para los funcionarios y se podrá convertir en un incumplimiento del contrato respecto de los contratistas, que pueda dar lugar a la imposición de sanciones e incluso su terminación, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.

6.3 ASPECTOS ORGANIZATIVOS DE LA GESTIÓN DE ACTIVOS: INVENTARIO DE ACTIVOS DE INFORMACIÓN

La identificación del inventario de activos de información, permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso.

6.3.1 DECLARACIÓN

Activos de Información es cualquier elemento que recopile, almacene, procese o distribuya la información en la entidad y que tenga valor para la misma.

Los Activos de Información son todo aquello que UNITECNAR, considera importante o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos, usuarios, contraseñas, etc.

En general es toda la información que la entidad posee dentro de un activo informático tales como servidores, Bases de Datos, Sistemas de Información, etc.

6.3.2 RESPONSABILIDAD DE LOS ACTIVOS DE INFORMACIÓN.

Se identifican los activos de información de mayor importancia, con sus responsables y su ubicación, para luego elaborar un inventario con dicha información.

El Inventario se deberá identificar, documentar y actualizar ante cualquier modificación de la información y los Activos asociados con los Medios de Procesamiento. Este debe ser revisado con una periodicidad no mayor a un (1) año.

La responsabilidad de realizar y mantener actualizado el inventario de activos de información es de cada responsable de proceso de UNITECNAR, en compañía del Líder de Seguridad de la Información.

El uso de los activos de información pertenecientes a UNITECNAR, es responsabilidad del propietario asignado; es su deber proteger y mantener la confidencialidad, integridad y disponibilidad de los activos de información.

6.4 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

El objetivo de asignar usuarios corresponde a establecer el acceso a los diferentes recursos tecnológicos de la institución, a todas aquellas personas que formen parte de la misma, otorgándole el derecho y privilegio de inicio de sesión en la red institucional.

La División de Tecnología y Sistemas de Información deberá:

- Recibir las solicitudes de creación o modificación de usuarios por parte de la División de Talento Humano.
- Crear el usuario de nuevos colaboradores con la finalidad de darle acceso a los diferentes recursos tecnológicos a los cuales tendrá permiso.
- Asegurarse que las cuentas de usuarios creadas para usuarios externos a la institución siempre serán de tipo temporal.
- Deshabilitar los usuarios de los empleados que hayan finalizado su contrato laboral según información remitida por División Talento Humano.

Responsabilidades de los Usuarios:

- Ningún usuario podrá solicitar directamente a la División de Tecnología Sistemas de Información, la creación de acceso a la red institucional ni a los diferentes sistemas de información.
- Debe asegurarse de cerrar de manera correcta todas las sesiones de usuarios abiertas al momento de finalizar su jornada laboral.
- No permitir a personas ajenas a la institución, el acceso a los diferentes recursos tecnológicos asignados.

6.5 CONTROL DE ACCESO.

La principal Base de Datos institucional la gestiona un Sistema de Información llamado ACRATE. Esta gestión garantiza la seguridad y disponibilidad de la información para el software de manejo de REGISTROS ACADEMICOS, ADMINISTRATIVOS Y FINANCIEROS, que es un sistema de información privado que posee UNITECNAR, desde el año 2005, permanece actualizado y con contrato vigente para garantizar los requerimientos normativos y los mantenimientos y actualizaciones respectivos.

Toda la documentación relacionada con los sistemas de UNITECNAR, es considerada confidencial y no debe ser conservada por los colaboradores que dejen de laborar en la empresa. En casos especiales y bajo solicitud expresa del jefe inmediato, se conservará una copia de seguridad de la información al momento de su retiro definitivo de la entidad.

6.6 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

La Oficina de TECNOLOGIAS Y SISTEMAS DE INFORMACION cuenta con personal con responsabilidad técnica para cada sistema de información.

Un Profesional en Sistemas presta el mantenimiento para las bases de datos del sistema de seguridad de la información.

La entidad cuenta con un equipo de Ingenieros desarrolladores que atiende los requerimientos puntuales, SOLICITUD DE ACTUALIZACIÓN, DESARROLLO O ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN, de acuerdo a las necesidades identificadas que son tenidas en cuenta por la Gerencia para su planeación y ejecución.

6.7 PROTECCIÓN CONTRA SOFTWARE NOCIVO

- Cualquier usuario quien sospeche de una infección por un virus debe apagar inmediatamente el computador involucrado, desconectarlo de cualquier red, llamar al grupo de soporte de la división de tecnologías y sistemas de información y no hacer ningún intento de eliminar el virus.

- Solamente el grupo de soporte de la oficina de la división de tecnologías y sistemas de información debe enfrentar una infección por virus de computador. Los usuarios no deben intentar eliminar el virus, a menos que sigan instrucciones precisas de los Administradores de sistemas.

- Los usuarios no deben transferir (bajar) software desde cualquier sistema que se encuentra por fuera de UNITECNAR.

- Los usuarios no deben utilizar software obtenido externamente desde Internet o de una persona u organización diferente a los distribuidores confiables o conocidos, a menos que el software haya sido examinado en busca de código malicioso y que haya sido aprobado la Oficina de Sistemas.

- Siempre que algún software o archivos hayan sido recibidos de una entidad externa, este material debe ser probado para buscar software no autorizado en una máquina aislada (no producción), antes de ser utilizado en los sistemas de información de UNITECNAR.

- Debe certificarse que todo el software, archivos o ejecutables, se encuentran libres de virus antes de ser enviados a una entidad externa a UNITECNAR.

- Cualquier archivo encriptado suministrado por instituciones externas a UNITECNAR, debe ser des encriptado antes de ser sometido al análisis con sistemas antivirus.

- Cualquier sistema de almacenamiento como CD-ROMs, unidades ópticas, cintas DAT, etc., provistos por instituciones externas deben ser verificados por los sistemas de antivirus de UNITECNAR

- Antes que cualquier archivo sea restaurado en un sistema de UNITECNAR, desde un medio de almacenamiento de respaldo, éste debe ser analizado con un sistema antivirus actualizado.

6.8 PROTECCIÓN DURANTE LA NAVEGACION EN INTERNET.

El servicio de navegación podrá ser utilizado por estudiantes, docentes, administrativos y visitantes autorizados.

El Director de Tecnología, se reserva el derecho de restringir el acceso a páginas web que, de acuerdo con las políticas institucionales, no deban ser vistas por los usuarios de la institución, así como las páginas y servicios cuya utilización afecte considerablemente el rendimiento del ancho de banda del enlace a Internet y que no sean relevantes para el desarrollo de las actividades académico-investigativas de la institución o puedan afectar la seguridad de los servicios o la información.

Está prohibido la transmisión y/o descarga de material obsceno o pornográfico, material que contenga amenazas o cualquier tipo de información que atente contra la moral o buenas costumbres.

No usar aplicaciones VPN que es permita ingresar a los diferentes sitios bloqueados

por el área de tecnología. Los colaboradores y clientes deberán abstenerse de brindar cualquier tipo de información de la institución en sitios no autorizados o que no cuenten con mecanismos de seguridad que garanticen la confidencialidad de la información en tránsito.

Los colaboradores de UNITECNAR, no deben comprar bienes o servicios a través de Internet a nombre de UNITECNAR, a menos que exista una aprobación previa.

Los usuarios, deben evitar descargar y/o emplear archivos de imagen, sonido o similares que puedan estar protegidos por derechos de autor de terceros sin la previa autorización de los mismos.

Los usuarios no deben descargar software de Internet bajo ninguna circunstancia. Los usuarios no deben instalar software en sus estaciones de trabajo, en los servidores de la red, o en otras máquinas, incluso si este software es libre o no licenciado; toda instalación de software debe hacerla un técnico luego de la debida verificación y la autorización de Sistemas.

Los usuarios están conscientes de que toda la información (incluida la de navegación) que transite en la institución por ser para el trabajo es propiedad de la misma y por ende puede ser monitoreada con objetivos de administración, seguridad o auditoría por personal autorizado por la Institución.

Los usuarios de los sistemas de navegación son conscientes de que estos, solamente deben ser utilizados para propósitos lícitos y en cumplimiento de las funciones específicas de su cargo, ya que toda actividad de navegación puede ser registrada por UNITECNAR, quien podrá revelar cualquier acceso cuando una autoridad judicial así lo requiera.

La Institución facilita el acceso al uso de medios electrónicos para comercio electrónico como el pago de facturas, transacciones bancarias de sus colaboradores y lectura de correos personales que tengan acceso vía web, pero no asume ninguna responsabilidad por estas, ni recomienda su uso.

6.9 SEGURIDAD DEL CORREO ELECTRÓNICO

La FUNDACION UNIVERSITARIA ANTONIO DE AREVALO UNITECAR asigna,

por medio de la División de Tecnología, Sistemas de Información un correo electrónico institucional para estudiantes, egresados, docentes y administrativos mediante el dominio (unitecnar.edu.co) el cual tiene un espacio virtual de almacenamiento acordado previamente con el proveedor.

- El uso del correo electrónico debe ser orientado al rol correspondiente y no para actividades de carácter personal.
- La institución no se hace responsable del contenido de los correos o archivos alojados en el espacio virtual de almacenamiento.
- La División de Talento Humano solicitará la eliminación y suspensión de la cuenta del personal docente y administrativo que se retira de la institución, en caso de eliminación se transferirá los datos alojados a otra cuenta proporcionada por Talento Humano.
- La institución podrá cambiar el perfil o las credenciales de acceso de una persona para el servicio cuando lo considere necesario.
- La institución no se hace responsable de la información que los usuarios almacenen en su cuenta de correo institucional. Es responsabilidad de cada usuario tener copias de respaldo (BackUps) de todo el contenido que guarde en el servicio.
- Las cuentas de correo institucional, se basan en los servicios ofrecidos por la compañía Google y por ello hereda todas las políticas de estos, como la política de SPAM de correos entrantes y salientes, y la notificación a la administración de correo sobre las actividades irregulares de los usuarios.
- En caso de recibir reporte justificado por parte de Google u otra compañía o entidad sobre el mal uso del correo electrónico, se suspenderá temporalmente su uso y sí su comportamiento es reiterativo se suspenderá permanentemente, al menos que se reciba la notificación de acceso por parte de las directivas de la institución.

7 ESTRATEGIAS

7.1 ESTRATEGIA 1: ACTUALIZACIÓN DEL INVENTARIO DE ACTIVOSDE INFORMACIÓN

Actualizar el Inventario de Activos que contengan Información personal.

7.2 ESTRATEGIA 2: IDENTIFICACIÓN Y VALORACIÓN DE RIEGOS DE SEGURIDAD DE LA INFORMACIÓN

Identificación de los riesgos de Seguridad de la Información.

7.3 ESTRATEGIA 3: ESCOGER Y FORMALIZAR LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Seleccionar y definir los controles de seguridad de la información para UNITECNAR, entre los cuales se encuentran los siguientes:

7.3.1 Etiquetado y manejo de la información

Se deben desarrollar los medios para el Etiquetado y Manejo de la Información, de acuerdo al esquema de clasificación definido por UNITECNAR, Los mismos contemplarán los Activos de Tecnología de la información tanto en formatos Físicos, Digital, Activos Tecnológicos.

7.3.2 Escritorio limpio.

Para UNITECNAR, es crucial proteger información sensitiva, evitando que sea conocida por personas diferentes a aquellas que la requieren o que sea publicada de manera indiscriminada.

Teniendo presente que las oficinas son visitadas frecuentemente por proveedores, consultores, clientes, personal de limpieza y otros compañeros de trabajo, se define esta buena práctica que se traduce como mantener su escritorio lo más limpio y organizado posible, ya que, si está desordenado, es muy probable que usted no se

dé cuenta de que le hace falta algo.

La información de la institución deberá mantenerse disponible a las personas autorizadas para ello en el momento en que se necesite, lo que hace que información sensible se pueda encontrar en el puesto de trabajo de cada empleado durante su jornada, sin que esto deba ser entendido como admitir momentos en que la información NO esté debidamente protegida.

DURANTE LA JORNADA LABORAL

Los sistemas de información y elementos de procesamiento deberán ser adecuadamente protegidos, teniendo presente que se debe al menos guardar documentos sensibles o elementos de almacenamiento de información (CD, Memorias portátiles, Discos Portátiles, asistentes personales, portátiles) en los cajones bajo llave, en todo momento que no los esté utilizando.

Es responsabilidad de cada usuario la protección de los sistemas de información a su cargo, por lo que debe asegurar físicamente su computador portátil con cables de seguridad en todo momento para evitar robos.

- Nombre de Usuario y Claves.
- Direcciones IP
- Contratos
- Números de Cuenta
- Listas de Clientes
- Propiedad Intelectual
- Datos de Empleados
- Cualquier cosa que no desea publicar

DESPUES DE LA JORNADA LABORAL

Los usuarios de la empresa deberán tomarse el tiempo necesario antes de abandonar la oficina para recoger y asegurar el material sensible.

BLOQUEO DE SESION

Para la empresa es importante que una estación de trabajo se mantenga en control, aun cuando su usuario no se encuentre frente a ella, por lo que se requiere que se encuentra bloqueada cuando el usuario se retire de su lugar, pues el no hacerlo potencia el riesgo de utilizar los sistemas sin los privilegios adecuados, expone la información de la institución de manera innecesaria y se considera un uso inadecuado de los recursos.

Cada usuario de la institución para mantener su estación de trabajo bajo control, deberá bloquear la sesión al alejarse de su computador, aunque sea por poco tiempo, minimizando el tiempo que la estación quedaría sin control ya que cualquier ausencia puede extenderse.

7.4 ELABORAR LOS INDICADORES DE SEGURIDAD DE LA INFORMACIÓN Y REALIZAR LA MEDICIÓN

Definir los indicadores de seguridad de la información e iniciar su medición.

ACTIVIDADES: Realizar mesa de trabajo para seleccionar, definir, establecer e iniciar la medición de los indicadores de seguridad de la información.

MANEJO DE LA INFORMACIÓN

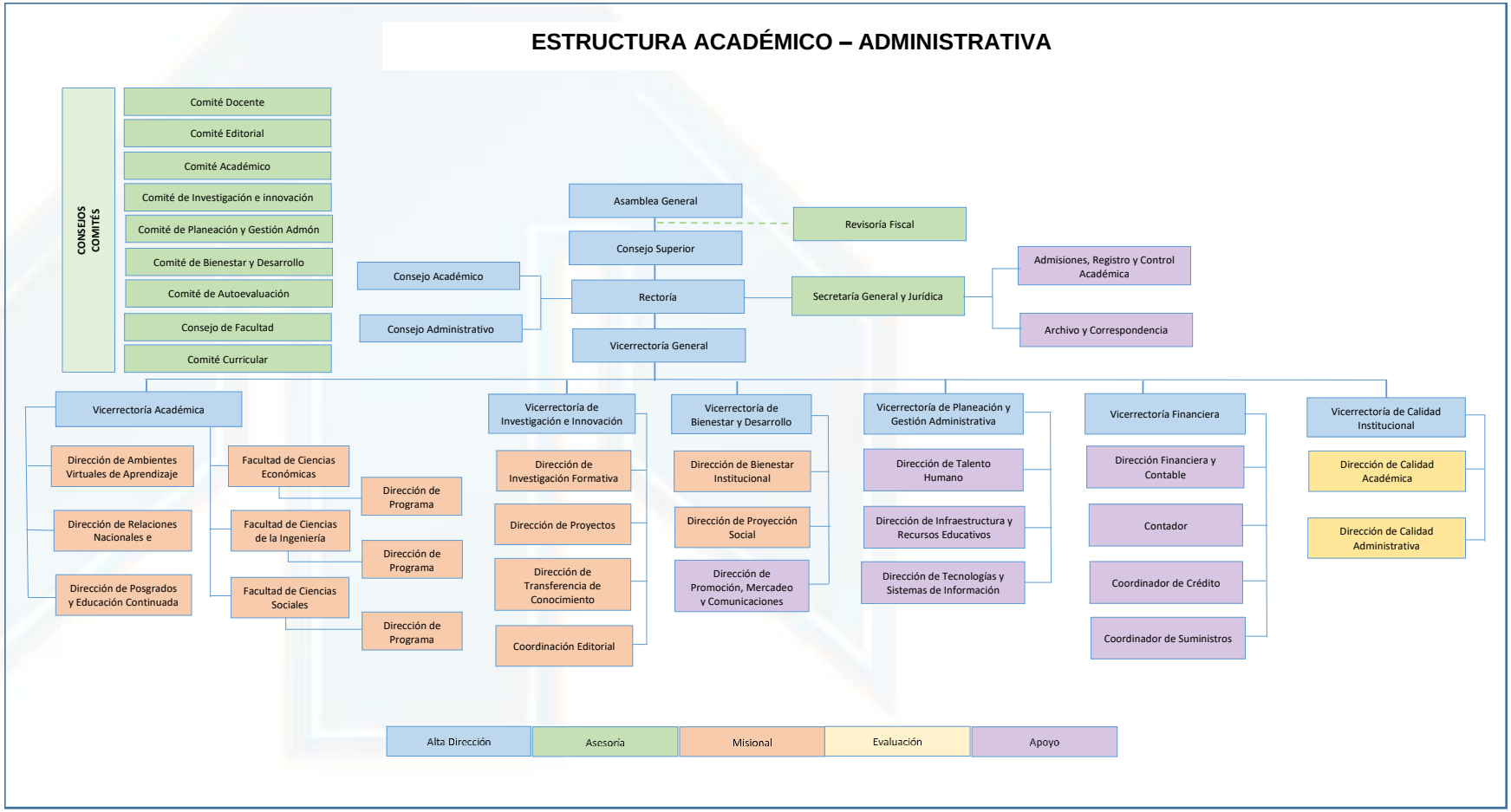
BACKUPS

- Será responsabilidad de La División de Tecnología Y Sistemas de Información realizar copia de seguridad de los servidores institucionales.
- Los usuarios deberán realizar las debidas copias de seguridad de la información institucional cada vez que lo requiera.
- Es responsabilidad de los administradores de los servidores de la institución, conocer, adoptar e implementar la presente política de Backup; también son los responsables de mantener actualizadas las políticas y procedimientos consignados en este documento.

- Es responsabilidad de cada usuario guardar toda su información (Archivos en 22xce, pdf, 22xcel, entre otros) en memorias USB, DVD, CD, o solicitar autorización para el almacenamiento en los servidores de la nube.
- Todos los días después de las 18:00 horas se hará backup de las bases de datos de la Fundación.
- Mensualmente se realizará copias de seguridad de la página web
- Realizar rutinas de seguimiento y control de backups.

8 ASPECTOS GENERALES

8.1 ESTRUCTURA ORGÁNICA



8.2 ROLES Y RESPONSABILIDADES

CARGO	ROL	RESPONSABILIDAD
Rectoría	Gerencia de la Información	Liderar las directrices del sistema de la seguridad de la información
Director de Tecnologías y Sistemas de Información	Participante Activo de la Gerencia de la Información	Velar por la implementación de las directrices de la Gerencia de la Información.
Vicerrector de Planeación y Gestión Administrativa	Oficial de Protección de Datos	Velar por la protección de los datos personales almacenados en las Bases de Datos Institucionales y por el cumplimiento de la normatividad vigente

9 DOCUMENTOS RELACIONADOS

DOCUMENTOS
POLITICA DE PROTECCION DE DATOS
INSTRUCTIVO PARA LA CREACIÓN Y ELIMINACIÓN DE USUARIOS Y CONTRASEÑAS