TI

Tecnología de Información –SISTEMAS-

UNIVERSIDAD UNIACC

Política de Seguridad Informática

ELABORÓ	REVISÓ	AUTORIZÓ
Miguel Said	Consejo Superior UNIACC	

POLÍTICAS DE SEGURIDAD INFORMÁTICA

PERSONAS

Los funcionarios y la seguridad informática

La responsabilidad por la seguridad de la información no sólo corresponde a las áreas de seguridad informática, sino que es una obligación de cada funcionario.

1.- Códigos de identificación y claves

1.1 Los mecanismos de acceso que les sean otorgados a los funcionarios son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona, a menos que exista un requerimiento legal o medie una procedimiento de custodia de llaves. De acuerdo con lo anterior, los usuarios no deben obtener las claves u otros mecanismos de acceso de otros usuarios que pueda permitirles un acceso indebido.

1.2 Los usuarios son responsables de todas las actividades llevadas a cabo con su código de usuario y clave personal.

2. Control de la Información

2.1 Los usuarios deben informar inmediatamente al área que corresponda dentro de la universidad toda vulnerabilidad encontrada en los sistemas, aparición de virus o programas sospechosos e intentos de intromisión y no deben distribuir este tipo de información interna o externamente.

2.2 Los usuarios no deben instalar software en sus computadores o en servidores sin las debidas autorizaciones.

2.3 Los usuarios no deben intentar sobrepasar los controles de los sistemas, examinar los computadores y redes de la universidad en busca de archivos de

otros sin su autorización o introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas.

2.4 Los funcionarios no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas. Esto incluye los controles del sistema de información y su respectiva implementación.

2.5 Los funcionarios no deben destruir, copiar o distribuir los archivos de la universidad sin los permisos respectivos.

2.6 Todo funcionario que utilice los recursos de los sistemas tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información ha sido clasificada como crítica.

3. Otros usos

3.1 Los computadores, sistemas y otros equipos deben usarse sólo para las actividades propias de la entidad, por lo tanto los usuarios no deben usar sus equipos para asuntos personales a menos que exista una autorización respectiva que avalúe el riesgo informático de tal labor.

3.2 La universidad debe tener definido un código de ética para la seguridad informática, el cual debe incluir tópicos relacionados con la seguridad informática y de datos.

SOFTWARE

Los empleados con funciones y responsabilidades para con el software institucional deben seguir los siguientes lineamientos para proteger este activo y la información que a través de él se maneje.

1. Administración del Software

1.1 La universidad debe contar en todo momento con un inventario actualizado del software de su propiedad, el comprado a terceros o desarrollado internamente, el adquirido bajo licenciamiento, el entregado y el recibido en comodato. Las licencias se almacenarán bajo los adecuados niveles de seguridad e incluidas en un sistema de administración, efectuando continuos muestreos para garantizar la consistencia de la información allí almacenada. Igualmente, todo el software y la documentación del mismo que posea la universidad incluirán avisos de derechos de autor y propiedad intelectual.

1.2 Todas las aplicaciones se clasificarán en una de las siguientes categorías: Misión Crítica, Prioritaria y Requerida. Para las de misión crítica y prioritaria deberá permanecer una copia actualizada y su documentación técnica respectiva, como mínimo en un sitio alterno y seguro de custodia.

1.3 Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad. Los programas que se encuentren en el ambiente de producción de la universidad, se modificarán únicamente por el personal autorizado, de acuerdo con los procedimientos internos establecidos y en todos los casos, y se considerarán planes de contingencia y recuperación.

2. Adquisición del Software

2.1 El software contará con acceso controlado que permita al propietario del recurso restringir el acceso al mismo. El software protegerá los objetos para que los procesos y/o los usuarios no los puedan acceder sin los debidos permisos. Cada usuario se identificará por medio de un único código de identificación de usuario y clave, antes de que se le permita el acceso al sistema.

3. Parametrización

3.1 Con el propósito de asegurar la integridad de la información, la función de Parametrización del software estará a cargo de un equipo interdisciplinario. Para el caso de aplicaciones de

misión crítica y prioritaria, el grupo interdisciplinario representará a los diferentes usuarios e incluirá al proveedor. Para el paso del software al ambiente de pruebas, el documento final de Parametrización del software contará previamente con las aprobaciones correspondientes al interior de la Universidad.

4. Desarrollo de Software

4.1 La universidad deberá tener una metodología formal para el desarrollo de software de los sistemas de información de misión crítica y prioritaria, desarrollos rápidos del mismo y las actividades de mantenimiento, las cuales cumplirán con las políticas, normas, procedimientos, controles y otras convenciones estándares aplicables en el desarrollo de sistemas. Los controles desarrollados internamente deberán ser como mínimo el plan de cuentas, el plan de auditoría y el cierre de puertas traseras. Adicionalmente, toda solicitud de modificación al software deberá contar con estudios de factibilidad y de viabilidad al igual que las autorizaciones respectivas dentro de la universidad.

4.2 Con el propósito de garantizar integridad y confidencialidad de la información que administrará el software desarrollado y antes del paso a pruebas, se deberán ejecutar las pruebas intrínsecas al desarrollo y a la documentación técnica respectiva. Para todo desarrollo de software se deberán utilizar herramientas, de las cuales se tengan certeza que su comportamiento es seguro y confiable. Solamente las funciones descritas en el documento aprobado de especificaciones de la solución tecnológica podrán ser desarrolladas

4.3 Los programadores de software no deberán conocer las claves utilizadas en ambientes de producción.

4.4 Los desarrollos y/o modificaciones hechos a los sistemas de aplicación no deberán trasladarse al ambiente de producción si no se cuenta primero con la documentación de entrenamiento, operación y de seguridad adecuados. La suficiencia de este material deberá ser determinada por los usuarios responsables en la universidad.

5. Pruebas de Software

5.1 Un equipo especializado deberá hacer las pruebas en representación de los usuarios finales. El área de desarrollo de sistemas deberá entregar el software desarrollado con códigos fuentes al área responsable de ejecutar las pruebas, el cual deberá ser revisado para encontrar

códigos mal intencionado y debilidades de seguridad utilizando preferiblemente herramientas automáticas, para luego ser compilado e iniciar las pruebas correspondientes.

5.2 Los tipos de pruebas deberán ser previamente establecidos. Para garantizar la integridad de la información en producción éstas deberán ser debidamente planeadas, ejecutadas, documentadas y controlados sus resultados, con el fin de garantizar la integridad de la información en producción. Además, el ambiente de pruebas deberá ser lo más idéntico, en su configuración, al ambiente real de producción.

5.3 Las pruebas sobre el software desarrollado tanto interna como externamente deberán contemplar aspectos funcionales, de seguridad y técnicos. Adicionalmente, se incluirá una revisión exhaustiva a la documentación mínima requerida, así como la revisión de los procesos de retorno a la versión anterior. En caso que se requirieran las claves de producción para ejecutar pruebas, su inserción y mantenimiento se deberá efectuar de manera segura. Se deberá poseer un cronograma para la ejecución de las pruebas con el fin de cumplir con los compromisos institucionales acordados. Éste podrá verse afectado en su calendarización por aquellos eventos en que se tengan que atender desarrollos rápidos únicamente por exigencias mandatorias de entes superiores.

6. Implantación del Software

6.1 Para implantar un software mediará una autorización por escrito del responsable para tal fin. Las características que son innecesarias en el ambiente informático se identificarán y desactivarán en el momento de la instalación del software.

6.2 Antes de implementar el software en producción se verificará que se haya realizado la divulgación y entrega de la documentación, la capacitación al personal involucrado, su licenciamiento y los ajustes de parámetros en el ambiente de producción. Deberá existir un cronograma de puesta en producción con el fin de minimizar el impacto del mismo.

6.3 Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área asignada para tal efecto, que en ningún momento deberá ser el área de desarrollo ni la de producción.

6.4 Los programas en el ambiente de producción serán modificados únicamente por personal autorizado y cuando se requiera por fuerza mayor de acuerdo con las normas institucionales establecidas.

7. Mantenimiento del Software

7.1 El área de desarrollos de sistemas no hará cambios al software de producción sin las debidas autorizaciones por escrito y sin cumplir con los procedimientos establecidos. A su vez, se contará con un procedimiento de control de cambios que garantice que sólo se realicen las modificaciones autorizadas.

7.2 La documentación de todos los cambios hechos al software se preparará simultáneamente con el proceso de cambio. Se deberá considerar, además, que cuando un tercero efectúe ajuste al software, éste deberá firmar un acuerdo de no-divulgación y utilización no autorizada del mismo.

7.3 Para cada mantenimiento a la versión del software de misión crítica y prioritaria se actualizará el depositado en custodia en el sitio alterno y el respaldado en la institución. Este software y su documentación se verificará y certificará su actualización.

DATOS

Los funcionarios de la universidad son responsables de la información que manejan y deberán seguir los siguientes lineamientos para protegerla y evitar pérdidas, accesos no autorizados y utilización indebida de la misma.

1. Clasificación de la Información

1.1 Todos los datos de propiedad de UNIACC se deben clasificar dentro de las siguientes categorías para los datos sensibles: SECRETO, CONFIDENCIAL, PRIVADO, y para los datos no sensibles la categoría es PÚBLICO. Para identificar la naturaleza de la información y las personas autorizadas para accesarla se deben utilizar prefijos como indicadores generales tales como: 'Financiero', 'Administrativo', 'Comercial', 'Jurídico', 'Tecnológico'. Toda información secreta, confidencial y privada debe etiquetarse según las normas de UNIACC, y todos los datos que se divulguen por cualquier medio deben mostrar la clasificación de sensibilidad de la información.

1.2 Cuando se consolidad información con varias clasificaciones de sensibilidad, los controles usados deben proteger la información más sensible y se debe clasificar con el máximo nivel de restricción que contenga la misma.

1.3 La información que se clasifica dentro de las categorías de sensibilidad debe identificarse con la marca correspondiente y se debe indicar la fecha en que deja de ser sensible, esto aplica para la información que se reclasifica tanto en un nivel inferior como en un nivel superior de sensibilidad.

1.4 La responsabilidad para definir la clasificación de la información debe ser tanto del dueño de la información como del área encargada de la seguridad informática en UNIACC.

1.5 La eliminación de la información debe seguir procedimientos seguros y debidamente aprobados por el responsable de la seguridad informática y de datos en la entidad.

2 Almacenamiento de la Información

2.1 Almacenamiento Masivo y Respaldo de Información

2.1.1 Toda información secreta debe estar encriptada, ya sea que se encuentre al interior de UNIACC o externamente, en cualquier medio de almacenamiento, transporte o transmisión.

2.1.2 Toda información sensible debe tener un proceso periódico de respaldo, tener asignado un período de retención determinado, la fecha de la última modificación y la fecha en que deja de ser sensible o se degrada. Sin embargo, la información no se debe guardar indefinidamente por lo cual se debe determinar un período máximo de retención para el caso en que no se haya especificado este tiempo.

2.1.3 La información clasificada como sensible (secreta, confidencial o privada) debe tener un respaldo, además debe tener copias recientes completas en sitio externo a UNIACC, en un lugar lejano de donde reside la información origen.

2.1.4 Todos los medios físicos donde la información de valor, sensitiva y crítica sea almacenada por períodos mayores a seis meses (6), no deben estar sujetos a una rápida degradación o deterioro.

2.1.5 Los respaldos de información de valor o sensible debe tener un proceso periódico de validación con el fin de garantizar que no ha sufrido ningún deterioro y que se podrá utilizar en el momento en que se necesite.

2.1.6 Toda la información contable, de impuestos y de tipo legal debe ser conservada de acuerdo con las normas y leyes vigentes.

2.2 Almacenamiento en forma impresa o documentos en papel

2.2.1 La remisión de información sensible tanto por correo interno como externo debe cumplir con los procedimientos establecidos de manera que se realice en forma segura.

2.2.2 Para todos los mensajes remitidos en formato libre de texto que contengan información sensible para el negocio debe numerarse cada línea y los

documentos oficiales de la entidad que se realicen a mano deben ser escritos con tinta.

2.2.3 Todas las copias de documentos secretos deben ser numeradas individualmente con un número secuencial para que las personas responsables puedan localizar rápidamente los documentos e identificar algún faltante de la misma.

3 Administración de la Información

3.1 Cualquier tipo de información interna de la entidad do debe ser vendida, transferida o intercambiada con terceros para ningún propósito diferente al del negocio y se debe cumplir con los procedimientos de autorización internos para los casos en que se requiera.

3.2 Todos los derechos de propiedad intelectual de los productos desarrollados o modificados por los empleados de la institución, durante el tiempo que dure su relación laboral, son de propiedad exclusiva de UNIACC.

3.3 Los datos y programas de UNIACC deben ser modificados únicamente por personal autorizado de acuerdo con los procedimientos establecidos, al igual que el acceso a bodegas de información debe restringirse únicamente a personal autorizado.

3.4 Cuando la información sensible no se está utilizando se debe guardar en los sitios destinados para eso, los cuales deben contar con las debidas medidas de seguridad que garanticen su confidencialidad e integridad.

3.5 En cualquier momento, el propietario de la información con la participación del responsable de la seguridad informática y de datos puede reclasificar el nivel de sensibilidad inicialmente aplicado a la información.

3.6 El acceso a la información secreta se debe otorgar únicamente a personas específicas.

3.7 Toda divulgación de información secreta, confidencial o privada a terceras personas debe estar acompañada por un contrato que describa explícitamente qué información es restringida y cómo puede o no ser usada.

3.8 Toda la información de la organización debe contemplar las características de Integridad, Confidencialidad, Disponibilidad, Auditabilidad, Efectividad, Eficiencia, Cumplimiento y Confiabilidad.

3.9 Todo software que comprometa la seguridad del sistema se custodiará y administrará únicamente por personal autorizado.

3.10 La realización de copias adicionales de información sensible debe cumplir con los procedimientos de seguridad establecidos para tal fin.

3.11 La información de UNIACC no debe ser divulgada sin contar con los permisos correspondientes, además, ningún empleado, contratista o consultor debe tomarla cuando se retire de UNIACC.

3.12 Todos los medios de almacenamiento utilizados en el proceso de construcción, asignación, distribución o encriptación se deben someter a un proceso de eliminación inmediatamente después de ser usados.

3.13 Toda la información histórica almacenada debe contar con los medios, procesos y programas capaces de manipularla sin inconvenientes, esto teniendo en cuenta la reestructuración que sufren las aplicaciones y los datos a través del tiempo.

4 Validaciones, controles y manejo de errores

4.1 Para reducir la probabilidad de ingreso erróneo de datos de alta sensibilidad, todos los procedimientos de ingreso de información deben contener controles de validación.

4.2 Se deben tener procedimientos de control y validaciones para las transacciones rechazadas o pendientes de procesar, además de tiempos determinados para dar la solución y tomar las medidas correctivas.

4.3 Todas las transacciones que ingresan a un sistema de producción computarizado, deben ser sujetos a un chequeo razonable, chequeos de edición y/o validaciones de control.

4.4 Todos los errores cometidos por los funcionarios de Uniacc y que son detectados por los usuarios deben cumplir con un proceso de investigación de acuerdo con los procedimientos y tiempos establecidos.

POLÍTICA DE HARDWARE

La administración, mantenimiento, modernización y adquisición de equipos computacionales y de telecomunicaciones debe adoptar los siguientes criterios para proteger la integridad técnica de la institución.

1. Cambios al Hardware

1.1 Los equipos computacionales de UNIACC no deben ser alterados ni mejorados (cambios de procesador, memoria o tarjetas) sin el consentimiento, evaluación técnica y autorización del área responsable (Soporte Computacional).

1.2 Los funcionarios deben reportar a los entes pertinentes de Uniacc sobre daños y pérdida del equipo que tengan a su cuidado y sea propiedad de Uniacc. La intervención directa para reparar el equipo debe estar expresamente prohibida. Uniacc debe proporcionar personal interno o externo para la solución del problema reportado.

1.3 Todos los equipos de la entidad deben estar relacionados en un inventario que incluya la información de sus características, configuración y ubicación.

1.4 Todo el hardware que adquiera la universidad debe conseguirse a través de canales de compra estándares.

1.5 Para todos los equipos y sistemas de comunicación utilizados en procesos de producción en la entidad, se debe aplicar un procedimiento formal de control de cambios que garantice que sólo se realicen los cambios autorizados. Este procedimiento de control de cambios debe incluir la documentación del proceso con las respectivas propuestas revisadas, la aprobación de las áreas correspondientes y la manera como el cambio fue realizado.

1.6 Todos los productos de hardware deben ser registrados por proveedor y contar con el respectivo contrato de mantenimiento.

1.7 Los equipos computacionales, sean estos PC, servidores, LAN, etc. no deben moverse o reubicarse sin la aprobación previa del Administrador o Jefe del área involucrada.

2 Acceso Físico y Lógico

2.1 Antes de conectarlos a la red interna todos los servidores de Intranet de Uniacc deben ser autorizados por el área responsable del hardware.

2.2 Todos los computadores multiusuario y los equipos de comunicaciones deben estar ubicados en lugares asegurados para prevenir alteraciones y usos no autorizados.

2.3 Las bibliotecas de cintas magnéticas, discos y documentos se deben ubicar en áreas restringidas en el DataCenter y en sitios alternos con acceso únicamente a personas autorizadas.

2.4 Todas las conexiones con los sistemas y redes de la entidad deben ser dirigidas a través de dispositivos probados y aprobados por la organización y contar con mecanismos de autenticación de usuario.

2.5 Los equipos de computación de Uniacc deben ser protegidos por mecanismos de control aprobados por el área de seguridad informática y de datos.

2.6 Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de Uniacc deben ser restringidas.

2.7 Todas las líneas que permitan el acceso a la red de comunicaciones o sistemas multiusuario deben pasar a través de un punto de control adicional (firewall) antes de que la pantalla de login aparezca en la terminal del usuario.

3 Respaldo y Continuidad del Negocio

3.1 La administración debe proveer, mantener y dar entrenamiento sobre los sistemas de protección necesarios para asegurar la continuidad del servicio en los sistemas de computación críticos, tales como sistemas de detección y eliminación de fuego, sistemas de potencia eléctrica suplementarios y sistemas de aire acondicionado, entre otros.

3.2 Los equipos del DataCenter se deben equipar con unidades suplementarias de energía eléctrica (UPS y Grupo Electrógeno).

3.3 El diseño de la red de comunicaciones debe estar de tal forma que se evite tener un punto crítico de falla, como un centro único que cause la caída de todos los servicios.

3.4 Los backups de los sistemas de computación y redes deben ser almacenados en una zona de fuego diferente de donde reside la información original. Las zonas de fuego varían de edificio a edificio y son definidas por el área de seguridad de Uniacc.

3.5 A todo equipo de cómputo, comunicaciones y demás equipos de soporte debe realizársele un mantenimiento preventivo y periódico, de tal forma que el riesgo a fallas se mantenga en una probabilidad de ocurrencia baja.

3.6 Los planes de contingencia y recuperación de equipos deben ser probados regularmente con el fin de asegurar que el plan sea relevante, efectivo, práctico y factible de realizar. Cada prueba debe documentarse y sus resultados y las acciones de corrección deben comunicarse a la alta dirección.

4 Otros

4.1 Ningún equipo portátil de computación debe registrarse como equipaje de viaje. Estos deben llevarse como equipaje de mano.

4.2 Los equipos portátiles de computación que contengan información sensible deben utilizar software de encriptación para proteger la información.

4.3 Todo equipo de cómputo y de comunicaciones de Uniacc debe tener un número (lógico y físico) de identificación permanente grabado en el equipo, además, los inventarios físicos se deben realizar en forma periódica, regular y eficiente.

4.4 Todo equipo portátil debe tener Declaración de Responsabilidad, la cual incluya instrucciones de manejo de información y acato de normas internas y de seguridad para el caso de robo o pérdida.

POLITICA DE INSTALACIONES FISICAS

Todos los funcionarios de Uniacc deberán seguir los siguientes lineamientos de seguridad física con el fin de salvaguardar los recursos técnicos y humanos de Uniacc.

1. Control de acceso físico

Uniacc debe contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control inteligente y sistemas de alarmas en las dependencias que se consideren críticas.

1.1 Personas

1.1.1 Los visitantes deben permanecer escoltados y portar un distintivo o escarapela claramente visible, y las personas que laboran para Uniacc que requieran ingresar a áreas críticas también deben permanecer escoltados. Además, tanto los visitantes como los empleados mencionados únicamente deben tener la información y recursos necesarios para el desarrollo de sus actividades.

1.1.2 En el evento que los funcionarios dejen de tener vínculos laborales con la entidad todos sus códigos de acceso deben ser cambiados o

desactivados. Además, en caso de pérdida de la escarapela o tarjeta de acceso también deben desactivarse dichos códigos.

1.1.3 Se debe mantener el registro de acceso del personal autorizado y de ingresos con el objeto de facilitar procesos de investigación.

1.1.4 Como mecanismo de prevención todos los empleados y visitantes no deben comer, fumar o beber en el DataCenter o en instalaciones con equipos tecnológicos. Al hacerlo estarían exponiendo los equipos a daños eléctricos como a riesgos de contaminación sobre los dispositivos de almacenamiento.

1.1.5 Las reuniones de trabajo donde se discute y maneja información sensible, se deben realizar en salas cerradas para que personas ajenas a ella no tengan acceso.

1.1.6 Todos los sistemas de control de acceso deben ser monitoreados permanentemente.

1.2 Equipos y otros recursos

1.2.1 Toda sede y equipo informático, ya sean propios o de terceros, que procesen información para Uniacc o posean un vínculo especial con la misma, debe cumplir con todas las normas de seguridad física que se emitan, con el fin de evitar el acceso a personas no autorizadas a las áreas restringidas donde se procese o mantenga información secreta, confidencial y privada, y asegurar la protección de los recursos de la plataforma tecnológica y su información.

1.2.2 Los equipos computacionales no deben moverse o reubicarse sin la aprobación previa del Administrador del área involucrada.

1.2.3 Todos los equipos de propiedad de Uniacc no deben retirarse de las instalaciones físicas por ningún personal, a menos que esté previamente autorizado.

1.2.4 No se debe proveer información sobre la ubicación del DataCenter o de los lugares críticos, como mecanismo de seguridad.

2 Protección física de la información

2.1 Todas las personas que trabajen para la entidad y/o aquellas designadas por las entidades para trabajar en actividades particulares (consultores y contratistas) son responsables del adecuado uso de la información suministrada para tal fin, por lo cual se debe velar por su integridad, confidencialidad, disponibilidad y auditabilidad. Toda información secreta, confidencial y privada debe estar provista de la seguridad necesaria por quien la maneja para evitar el uso indebido por parte de personal no autorizado.

2.2 Al terminar la jornada laboral, los escritorios y áreas de trabajo deben quedar desprovistos de documentos sensibles que puedan comprometer los intereses de Uniacc. Estos deben quedar bajo llave en archivadores, cajas fuertes o demás medios de almacenamiento físico seguros.

2.3 Las áreas donde se maneja información confidencial o crítica deben contar con cámaras que registren las actividades realizadas por los funcionarios.

3 Protección contra desastres

Dado que cualquier tipo de desastre natural o accidental ocasionado por el hombre puede afectar el nivel de servicio y la imagen de Uniacc, se deba prever que los equipos de procesamiento y comunicaciones se encuentren localizados en áreas aseguradas y debidamente protegidas contra inundaciones, robos, interferencias electromagnéticas, fuego, humo y demás amenazas que puedan interferir con el buen uso de los equipos y la continuidad del servicio.

4 Planes de emergencia, contingencia y recuperación

4.1 Es responsabilidad de la administración de Uniacc el preparar, actualizar periódicamente y regularmente probar los planes de Contingencias, Emergencias y Recuperación previendo la continuidad de los procesos críticos para el negocio en el evento de presentarse una interrupción o degradación del servicio.

4.2 La Administración debe establecer, mantener y probar periódicamente el sistema de comunicación que permita a los usuarios de la plataforma tecnológica notificar posibles intromisiones a los sistemas de seguridad, estos

incluyen posibles infecciones por virus, intromisión de hackers, divulgación de información no autorizada y debilidades del sistema de seguridad.

4.3 El Plan de Contingencia y de Recuperación debe permanecer documentado y actualizado de manera tal que sea de conocimiento general y fácilmente aplicable en el evento de la presencia de un desastre , permitiendo que los recursos previstos se encuentren disponibles y aseguren la continuidad de los procesos de negocio, en un tiempo razonable para cada caso y contemplando como mínimo los riesgos más probables de ocurrencia que afecten su continuidad.

4.4 El mantenimiento del plan de Contingencias y Recuperación general debe incluir entre otros un proceso estándar que integre los planes de contingencia para computadores y comunicaciones, así como también el inventario de hardware, software existente y los procesos que correrán manualmente por un período de tiempo.

POLITICA DE ADMINISTRACION DE SEGURIDAD INFORMÁTICA

1. Generalidades

1.1 El área de Seguridad Informática debe definir, implementar, controlar Y mantener las políticas, normas, estándares, procedimientos, funciones y responsabilidades necesarias para preservar y proteger la confidencialidad, disponibilidad e integridad de la información de Uniacc donde ésta resida (aplicaciones, bases de datos, sistemas operativos, redes, backups y medios).

1.2 El área de Seguridad Informática es la encargada de establecer, mantener y administrar una arquitectura de seguridad para Uniacc y facilitar la incorporación de prácticas de seguridad de la información en todas las dependencias.

1.3 El área de seguridad Informática debe estar ubicada organizacionalmente de manera que tenga autonomía e independencia frente a las demás áreas de tecnología tales como soporte, diseño y desarrollo, entre otras.

1.4 Promover que los planes estratégicos y de operaciones de Uniacc estén alineados con las estrategias de seguridad de Uniacc.

1.5 El área de seguridad debe velar porque las excepciones a las políticas de seguridad estén autorizadas únicamente por la Dirección Superior, y se debe dejar constancia de los riesgos que en forma consciente se están asumiendo y el período de vigencia de la excepción.

2 Funciones de Control

2.1 Establecer e implementar un plan de Seguridad que permita controlar el entorno lógico y físico de la información estratégica de Uniacc, teniendo en cuenta criterios de confidencialidad, integridad, auditabilidad, disponibilidad, autenticidad de la información.

2.2 Participar activamente en los proyectos informáticos de la entidad para proveerlos de las seguridades adecuadas, gerenciando los de Seguridad Informática.

2.3 Definir las directrices básicas de Seguridad Informática para la descripción de los diferentes requerimientos en la adquisición de tecnología (hardware y software) en Uniacc, y velar porque se realicen las pruebas de seguridad a los Sistemas de Información.

2.4 Participar activamente en el equipo de trabajo de análisis, implementación y mantenimiento de los perfiles de usuario que interactúan con los Sistemas Operativos, Bases de Datos y Aplicaciones, y velar porque en producción únicamente estén los autorizados y vigentes.

2.5 Contar con mecanismos de monitoreo con el fin de detectar oportunamente procedimientos inseguros para los Sistemas Operacionales, Aplicaciones, Datos y Redes.

2.6 Desarrollar métodos y técnicas para monitorear efectivamente los sistemas de seguridad de la información y reportar periódicamente su efectividad a la Dirección de TI.

2.7 Direccionar, recomendar y aconsejar a todos los usuarios de los sistemas de Uniacc en cuanto a la seguridad de la información.

2.8 Interactuar con los organismos de control interno y externo, apoyándolos en su gestión administrativa y de ejecución.

2.9 Asegurar que la organización cuente con ambientes independientes de Desarrollo, Pruebas, Producción y Capacitación.

2.10 Garantizar que todos los mantenimientos a los sistemas de misión crítica y prioritaria estén autorizados, probados e implementados de acuerdo con los requerimientos de los usuarios previamente validados por un grupo especializado y que no comprometan la seguridad informática de la organización. Además, que los sistemas de información queden correctamente documentados y se dé la capacitación a los usuarios finales.

2.11 El Área de Seguridad Informática es responsable por la revisión continua de las Políticas de Seguridad Informática por lo menos una vez al año.

3 Comité de Seguridad Informática

Conformar y liderar un Comité de Seguridad Informática en el cual se sustente el Plan de Seguridad Informática a ejecutar en Uniacc desarrollado por el área. Este comité debe analizar la administración de problemas de seguridad y se definan las estrategias a implementar que permitan controlar el entorno lógico y físico de la información estratégica de Uniacc.

4 Soporte a Investigaciones

4.1 Soportar las investigaciones sobre violaciones a la seguridad de los sistemas en apoyo al área de Seguridad no Tecnológica (Física) y presentar los informes respectivos a la Dirección Superior.

4.2 Investigar, documentar e informar a los propietarios de la información los incidentes de seguridad tanto lógica como física.

4.3 Realizar seguimiento a las acciones disciplinarias y legales asociadas con los incidentes de seguridad investigadas.

5 Elaboración del Mapa de Riesgos

5.1 Efectuar estudios de análisis de riesgos en Seguridad Informática para identificar oportunamente los eventos o situaciones de fallos en los accesos en el manejo de la información presentados en Uniacc, estableciendo planes de

acción que incluyan controles para contrarrestarlos y reducir el riesgo a un nivel aceptable.

6 Plan de Contingencia

6.1 Preparar, implementar y mantener el Plan de Contingencia y de Recuperación de desastres y continuidad del negocio relacionados con tecnología informática.

6.2 Liderar el proceso de pruebas que se debe ejecutar periódicamente a los Planes de Contingencia y de Recuperación.

7 Capacitación y Entrenamiento

7.1 Establecer y apoyar a las áreas encargadas en la ejecución de un plan de Capacitación continuo que permita actualizar a los funcionarios en aspectos de seguridad informática fortaleciendo la cultura sobre el tema.

7.2 Dar un entrenamiento adecuado a los usuarios, custodios y usuarios dueños de la información en cuanto a los requerimientos y responsabilidades sobre la seguridad de la información.

POLÍTICA DE SEGURIDAD INFORMÁTICA

CONTROL DE CAMBIOS Y MEJORAS

NIVEL DE REVISIÓN	SECCIÓN Y/O PÁGINA	DESCRIPCIÓN DE LA MODIFICACIÓN Y MEJORA	FECHA MODIFICACIÓN
01		Creación	Junio 2009
02			
03			
04			
05			

Aprobó	**Aprobó**	**Aprobó**
Miguel Said	Consejo Superior	