PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IFINORTE 2024

Tabla de contenido

INTRODUCCION

El Instituto Financiero para el Desarrollo de Norte de Santander IFINORTE, tiene clara la importancia de definir controles para preservar la confidencialidad, integridad y disponibilidad de la información que se gestiona en los procesos y a través de los procedimientos, por lo que se tomó la decisión de aplicar políticas de seguridad que minimicen los riesgos que amenacen y vulneren la información, con el fin de dar continuidad a sus servicios.

La seguridad de datos es un tema de gran importancia que nos involucra y afecta a casi todos hoy en día. Cada vez son más los productos tecnológicos que de alguna u otra manera deben ser tenidos en cuenta para temas de seguridad y que se están introduciendo en nuestra vida diaria. No solo hablamos de dispositivos conectados, también de App que crean nuevas “conexiones” entre ellos mismo, con interfaces o infraestructuras privadas, que terminan llevando información a las nubes, lo que a su vez crea más oportunidades para que los hackers puedan obtener dicha información. Todo esto ha impulsado una demanda de soluciones y expertos en seguridad de datos que sean capaces de construir redes más fuertes y menos vulnerables.

1.OBJETIVOS

1.1 Objetivo general

Establecer un plan de seguridad que permitan proteger la Información del Instituto Financiero para el Desarrollo de Norte de Santander IFINORTE, por medio de estrategias de aseguramiento de la Información teniendo en cuenta los requerimientos tecnológicos, operativos y de seguridad necesarios, alineados con el actual direccionamiento estratégico con el fin de garantizar el cumplimiento de la integridad, disponibilidad, legalidad y confidencialidad de la información.

1.2 Objetivos específicos

- Identificar y aplicar tecnologías encaminadas a fortalecer la seguridad de la información.
- Establecer planes que permitan una adecuada identificación y mitigación de los riesgos en relación al manejo de información en IFINORTE.
- Concientizar a los funcionarios, contratistas y demás personal relacionado de IFINORTE sobre el adecuado uso de la información puesta a su disposición para la ejecución de sus funciones y actividades diarias, garantizando la confidencialidad, privacidad e integridad de la misma.
- Obtener y mantener la confianza de los clientes, contando con el compromiso de los funcionarios, contratistas y demás personal relacionado con el Instituto respecto al adecuado manejo y protección de la información que es gestionada y resguardada por IFINORTE.
- Identificar y dar solución a las necesidades que permitan el cumplimiento de la función administrativa dentro de la entidad.
- Atender y dar seguimiento a los lineamientos establecidos por entidades como el MinTIC y la Superintendencia Financiera de Colombia.

2. ALCANCE

Por medio del presente documento se busca realizar un análisis de riesgos de seguridad de la información previamente identificada, determinando sus agentes o factores de amenaza, vulnerabilidad e impacto sobre los procesos de la entidad, dicha labor se realizará a través de un inventario de la información asociada a cada uno de los procesos de la entidad con el objetivo de determinar su nivel de criticidad, estableciendo un modelo que permita identificar las amenazas y vulnerabilidades a nivel tecnológico, por medio del uso de técnicas y herramientas de seguridad digital.

Las políticas de seguridad y privacidad de la información se aplicarán a todos los datos e información que reposen en IFINORTE que sean considerados confidenciales y/o críticos para los objetivos del negocio, los cuales pueden estar almacenados en forma electrónica y/o en forma física.

3. ANALISIS DE LA SITUACION ACTUAL

3.1 Personas

3.1.1 Códigos de Identificación Y Palabras Claves

La responsabilidad por la seguridad de la información no es únicamente de las áreas de seguridad informática, es una obligación de cada funcionario.

Las palabras claves o los mecanismos 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 un procedimiento de custodia de claves. De acuerdo con esto, los usuarios no deben obtener palabras claves u otros mecanismos de acceso de otros usuarios que pueda permitirles un acceso indebido.

El Control del sistema de información está especializado en detectar los intentos de acceso, permitiendo el paso de los usuarios autorizados, y denegando el paso a todos los demás tomando en cuenta las credenciales de ingreso que se tienen para cada uno de ellos. Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

3.1.2 Control De La Información

- Los usuarios deben informar inmediatamente al área de sistemas de la entidad 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.
- El personal de planta, contratistas y demás usuarios no deben instalar software en sus computadores o servidores sin las debidas previas autorizaciones.

- El personal de planta, contratistas y demás usuarios no deben intentar sobrepasar los controles de los sistemas debido a que hay credenciales dentro del árbol de exploración con usuarios ya definidos y permisos que posee cada usuario de manera independiente, el intento para realizar otro tipo de tarea es nulo por que el sistema no le permite ingresar a consultas que no están disponibles por control de seguridad e integridad de la información.

- Examinar los computadores y redes de la entidad en busca de archivos guardados sin previa autorización o software introducido intencionalmente diseñado para causar daño o impedir el normal funcionamiento de los sistemas.

- El personal de planta, contratistas y demás usuarios 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.
- El personal de planta, contratistas y demás usuarios no deben destruir, copiar o distribuir los archivos de la entidad sin los permisos previos respectivos.
- Las personas o clientes tienen derecho a bloquear su información para que no sea distribuida a terceros o incluida en listados del correo y hacer que la información de ellos sea borrada de las listas de mercadeo, por lo cual los funcionarios deben actuar de conformidad con lo anterior, guardando en todo momento la privacidad de la información del cliente.
- El personal de planta, contratistas y demás usuarios que utilicen los recursos informáticos, tienen la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información ha sido clasificada.

3.1.3 Otros Usos

Los equipos y dispositivos tecnológicos deben usarse solamente para las actividades propias de la entidad, por lo tanto, el personal de planta, contratistas y demás usuarios no deben usar sus equipos para asuntos personales a menos que exista una autorización respectiva que evalúe el riesgo informático de tal labor.

3.2 Software

El personal de planta, contratistas y demás usuarios con funciones y responsabilidades para con el software institucional deben seguir los siguientes lineamientos para proteger la información que a través de él se maneje:

- La Entidad debe contar en todo momento con un inventario actualizado del software de los equipos, 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 Entidad incluirán avisos de derechos de autor y propiedad intelectual.

- 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 Entidad, se modificarán únicamente por personal autorizado, de acuerdo con los procedimientos internos establecidos y en todos los casos, y se considerarán planes de contingencia y recuperación.

- El personal de planta, contratistas y demás usuarios que requieran la instalación de software que sea propiedad de IFINORTE, deberán justificar su uso y solicitar su autorización al área de sistemas con el visto bueno de su Jefe inmediato, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que será usado.

- Se considera una falta grave que el personal de planta, contratistas y demás usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red.

3.3 Datos

3.3.1 Clasificación de la Información

- Todos los datos de propiedad de la entidad se deben clasificar dentro de las siguientes categorías para los datos sensibles: RESTRINGIDA, CONFIDENCIAL, PRIVADA y para los datos no sensibles la categoría es PÚBLICO.

- La responsabilidad de definir la categoría en la que cada activo de información se encuentra es el responsable de la misma, así como determinar si con el paso del tiempo, el activo de información requiere una reclasificación.

- Toda la información debe tener un responsable, el cual asegure su correcta clasificación e implantación de controles para su protección.

- Por política general, toda la información que se maneja dentro de IFINORTE tiene carácter de CONFIDENCIAL hasta que se apruebe otro tipo de clasificación.

- 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.

3.3.2 Almacenamiento de la Información

3.3.2.1 Almacenamiento Masivo y Respaldo de Información

- Toda información sensible debe tener un proceso periódico de respaldo, tener asignado un periodo 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 periodo máximo de retención para el caso en que no se haya especificado este tiempo.

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

- 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.

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

- Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente en los equipos de cómputo administrativos y servidores.

- Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups.

- Conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las copias de respaldo, debidamente marcadas.

- Almacenamiento interno o externo de las copias de respaldo, verificando si se cuenta con custodia para ello.

- Las copias de seguridad o Back ups se deben realizar al menos una vez a la semana y el último día hábil del mes, el responsable del área de sistemas, revisará una vez por semana, el cumplimiento de este procedimiento y registrará en el formato de copias de seguridad.

3.3.2.2 Almacenamiento en forma impresa o documentos en papel

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.

3.3.3 Administración de la Información

- Cualquier tipo de información interna de la entidad no 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.

- Todos los derechos de propiedad intelectual de los productos desarrollados o modificados por el personal de planta, contratistas y demás usuarios de la Entidad, durante el tiempo que dure su relación laboral, son de propiedad exclusiva del Instituto.

- Los datos y programas de la entidad deben ser modificados únicamente por personal autorizado de acuerdo con los procedimientos establecidos.

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

- Toda divulgación de información restringida, 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.

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

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

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

- La información de la entidad no debe ser divulgada sin contar con los permisos correspondientes, además, el personal de planta, contratista, consultor o usuario no debe tomarla cuando se retire de la entidad.

3.3.4. Validaciones, controles y manejo de errores

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

- 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.

- Todos los errores cometidos el personal de planta, contratista o usuarios de la entidad y que son detectados por los clientes deben cumplir con un proceso de investigación de acuerdo con los procedimientos y tiempos establecidos.

- Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el área de Sistemas.

- Ningún miembro del personal de planta, contratista o usuarios de IFINORTE debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por el área de Sistemas.

- No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de IFINORTE.

4. POLITICA DE SEGURIDAD DE ACCESO A LA INFORMACION

4.1 Personas

En el evento que el personal de planta, contratista o usuarios dejen de tener vínculos laborales con IFINORTE todos sus códigos de acceso deben ser cambiados o desactivados.

Como mecanismo de prevención todo el personal de planta, contratista, usuarios o visitantes no deben comer, fumar o beber en el centro de cómputo o instalaciones con equipos tecnológicos, al hacerlo estarían exponiendo los equipos a daños eléctricos como a riesgos de contaminación sobre los dispositivos de almacenamiento.

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.

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

4.2 Equipos y Otros Recursos

Toda sede y equipo informático, ya sean propios o de terceros, que procesen información para la entidad 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.

Los equipos de cómputo no deben moverse o reubicarse sin la aprobación previa del Coordinador del área de Sistemas.

Todos los equipos propiedad del Instituto como computadores de escritorio, impresoras, teléfonos celulares, equipos portátiles, módems y equipos relacionados con sistemas de información NO deben retirarse de las instalaciones físicas por ningún personal, a menos que esté previamente autorizado.

No se debe proveer información sobre la ubicación del centro de cómputo, como mecanismo de seguridad.

4.3 Protección física de la información

Todas las personas que laboren para la entidad y/o aquellas designadas por las entidades para trabajar en actividades particulares (consultores, asesores 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 Reservada 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.

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

Las áreas donde se maneja información confidencial o crítica se cuenta con cámaras de seguridad que registran las actividades realizadas por los funcionarios.

5. POLITICA ADMINISTRACION DE SEGURIDAD INFORMATICA

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 la Entidad donde ésta resida (aplicaciones, bases de datos, sistemas operativos, redes, backups y medios).

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

Representar a la entidad ante organizaciones externas sobre temas de seguridad de la información.

Establecer e implementar un plan de Seguridad que permita controlar el entorno lógico y físico de la información estratégica de la entidad, teniendo en cuenta los criterios de confidencialidad, integridad, auditabilidad, disponibilidad, autenticidad y no repudiación de la información.

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

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.

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

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

6 POLITICA DE SEGURIDAD EN REDES DE COMUNICACIÓN

Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación de la entidad deberán ser tratadas como información confidencial.

El personal de planta, contratista o usuarios de IFINORTE no deben llevar a cabo

ningún tipo de instalación de líneas telefónicas, canales de transmisión de datos, módems, ni cambiar su configuración sin haber sido formalmente aprobados por el área responsable en la entidad.

Las centrales de conexión o centros de cableado deben ser catalogados como zona de alto riesgo, estos sitios se consideran zona roja con limitación y control de acceso.

El personal de planta, contratista o usuarios de IFINORTE no deben llevar a cabo ningún tipo de instalación a los canales de transmisión de datos, deben instalarse previa aprobación formal de las áreas responsables de la entidad.

6.1 Conexiones con redes públicas e Internet.

Toda conexión entre las redes de la entidad e Internet deberán contar como mínimo con mecanismos de control de acceso lógico, tales como, Firewall, proxys, DNS, entre otros; igualmente todos los usuarios deberán autenticarse ante estos mecanismos de seguridad; en caso de no contar con estos, la conexión a Internet deberá establecerse en un equipo independiente a la red de comunicaciones de la entidad.

Está prohibido toda conexión a través de módems a estaciones de trabajo que estén simultáneamente conectadas a una red de área local o a otra red de comunicación interna.

6.2 Servicios

Lo publicado en las páginas World Wide Web (WWW) debe ser autorizado por el ente competente.

El personal de planta, contratista o usuarios de IFINORTE que se enteren de la existencia de publicaciones con información de la Entidad en páginas no autorizadas, deben informar inmediatamente al área responsable.

El contenido de la página Web debe estar de acuerdo con las políticas de la entidad, debe tener medidas de seguridad y se debe ajustar a los estándares de diseño, navegación y redacción establecidos.

Con la excepción del correo electrónico, todos los accesos a Internet, deben ser aprobados previamente por el área responsable.

Los accesos a internet/Intranet para utilizar sistemas de información de la entidad en forma remota y en tiempo real deben ser autorizados por el área de seguridad informática.

El personal de planta, contratista o usuarios de IFINORTE no deben establecer carteleras electrónicas de anuncios en redes sociales, sin la previa autorización del área de seguridad informática.

6.3 Internet

Las leyes para derechos de reproducción, patentes, marcas registradas y todo lo relacionado con derechos de autor aplican en Internet.

Todo el software obtenido a través de Internet debe ser revisado por un software antivirus
(filtros de contenido), antes de transmitirlo internamente hacia usuarios del Instituto.

El uso de equipos y dispositivos tecnológicos de la entidad para tener acceso a Internet con fines personales no es permitido.

El personal de planta, contratista o usuarios de IFINORTE que accidentalmente se conecten a páginas de Internet que tengan contenidos sexuales, racistas o cualquier otro tipo de material ofensivo deben desconectarse inmediatamente e informar a su superior, para que sean bloqueados estos accesos.

6.4 Red

La información que se publique en la red de la entidad, debe contar con la aprobación del responsable del área encargada y la del propietario de la información involucrada.

El material que se publique en la red de la entidad debe ser revisado previamente para confirmar la actualidad, oportunidad e importancia de la información y evitar que los programas incluyan virus, así mismo se debe evaluar posibles problemas operativos y de seguridad de acuerdo a las políticas establecidas por el área de seguridad informática.

La información de la red debe ser únicamente utilizada por personal autorizado. El personal de planta, contratista o usuarios de IFINORTE no deben re direccionar información que aparezca en la red a terceros sin autorización de la entidad.

6.5 Correo Electrónico

El envío de mensajes masivos a través de correo electrónico debe ser realizado solo con aprobación de la gerencia.

El correo electrónico no debe ser utilizado por terceros (Clientes o proveedores) sin previa autorización.

La información confidencial no debe ser transmitida por correo electrónico, a menos que lo autorice la Gerencia.

El personal de planta, contratista o usuarios de IFINORTE no deben utilizar una cuenta de correo electrónico que pertenezca a otra persona, si hay necesidad de hacerlo en caso de ausencias o vacaciones se debe recurrir a mecanismos alternos como redirección de mensajes.

El personal de planta, contratista o usuarios de IFINORTE no deben enviar mensajes de correo electrónico con contendidos hostiles que molesten a los receptores del mismo, como comentarios sobre sexo, raza, religión o preferencias sexuales, así mismo cuando un empleado reciba este tipo de mensajes debe comunicarlo a su jefe inmediato y al área encargada de personal.

Ningún funcionario está autorizado para monitorear los mensajes de correo electrónico, excepto las áreas de control o áreas responsables. El monitoreo es realizado para cumplir con políticas internas en casos de sospechas de actividad no autorizada, investigaciones y otras razones de la alta gerencia, la entidad no está obligada a solicitar autorización del empleado involucrado.

El sistema de correo electrónico de la entidad debe ser usado únicamente para propósitos de trabajo.

Todos los mensajes enviados por este medio pertenecen a la entidad y ésta se reserva el derecho de accesar y revelar los mensajes enviados por este medio para cualquier propósito.

El personal de planta, contratista o usuarios de IFINORTE no deben utilizar versiones escaneadas de firmas hechas a mano para dar la impresión de que un mensaje de correo electrónico o cualquier otro tipo de comunicación electrónica ha sido firmada por la persona que la envía.

La entidad debe establecer normas para proteger la confidencialidad y privacidad de la información obtenida a través de sus servicios de correo electrónico, teniendo en cuenta

los siguientes parámetros: tipo de información que se obtiene, finalidad que se dará a la

información, modificación o actualización de la información, aceptación de los términos por las partes involucradas.

7. SEGURIDAD EN SISTEMAS DE INFORMACION Y SISTEMAS OPERATIVOS

7.1 Controles de acceso

Todos los sistemas automatizados deben utilizar estándares para los códigos de identificación de usuario, para nombres, programas y archivos tanto en ambientes de producción como en desarrollo, para nombres de sistemas de información y otras convenciones utilizadas en tecnología.

Toda transacción que afecte información de valor, sensible o crítica debe ser procesada únicamente cuando se valide la autenticidad del origen (usuario o sistema) y se compruebe su autorización mediante un mecanismo de control de acceso o perfiles.

Todo programa y archivo que contenga fórmulas, algoritmos u otras especificaciones que se utilicen para la generación de claves debe estar controlado con las más altas medidas de seguridad.

Ningún funcionario debe construir o utilizar mecanismos para coleccionar passwords o códigos de identificación de usuarios; ni tampoco mecanismos para identificar o autenticar la identidad de los usuarios sin la autorización del Área de Seguridad Informática.

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

7.2 Perfiles y privilegios

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los funcionarios que acceden al sistema, de tal forma que la información solo sea modificada por los usuarios autorizados y en los horarios establecidos.

Las modificaciones a los privilegios o perfiles de usuario deben ser realizadas por los usuarios finales, a través de pantallazos predefinidos para este fin.

Los privilegios especiales del sistema deben otorgarse únicamente a los funcionarios Administradores del Sistema o responsables de la seguridad. Los usuarios finales no deben tener acceso a los niveles de comandos para el funcionamiento del sistema.

Los Administradores de los Sistemas o súper-usuario deben tener por lo menos dos usuarios- IDs. Uno de acceso privilegiado y el otro debe ser un usuario-ID ordinario con

el que se lleve a cabo el trabajo diario de un usuario común.

El nivel de súper-usuario de los sistemas deben tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

Todas las herramientas de los sistemas de información, construidas o distribuidas por la entidad, que puedan usarse para causar un daño significativo deben ser automáticamente restringidas para que sean solamente usadas en el(los) propósito(s) determinado(s).

El hardware y software de diagnóstico y/o utilitarios sólo deberán ser usados por personal autorizado y su uso debe ser controlado por el área de seguridad informática en la entidad.

7.3 Controles automáticos y de usuario

El control de acceso a todos los equipos y dispositivos tecnológicos de la entidad debe realizarse por medio de códigos de identificación y palabras claves únicas para cada usuario.

Si el usuario digita un log-in (user id o clave) incorrecta, el sistema no debe mostrar la fuente del problema, simplemente debe informársele que el log-in es incorrecto y terminar la sesión o esperar un nuevo log-in.

Después de tres intentos consecutivos infructuosos al sistema, se debe suspender el acceso del usuario hasta que el administrador del sistema o responsable de la seguridad lo habilite de nuevo siguiendo con los procedimientos establecidos para identificación del usuario.

Las palabras clave deben tener la siguiente estructura: Longitud mínima de 8 Caracteres, de los cuales al menos un carácter alfabético en minúscula, otro en mayúscula, un carácter numérico y un carácter especial.

Los usuarios deben definir palabras claves que sean difíciles de adivinar, no pueden ser series de números (123456), ni repeticiones de caracteres (AAAA, 1111), ni situaciones familiares (fechas de cumpleaños, nombres familiares, placas del carro, etc.), ni palabras compuestas combinadas con cierto número de caracteres que cambian predeciblemente (na área, una fecha, una ciudad, un proyecto, etc.), ni palabras muy similares a otras definidas anteriormente.

El sistema debe llevar un histórico de palabras clave, de tal forma que los usuarios no usen palabras claves utilizadas anteriormente.

La identificación del usuario se debe asignar en forma secuencial y numérica de tal forma que no exista una relación obvia entre la identificación y el nombre verdadero del usuario.

Las palabras claves no se deben presentar en pantalla o impresas.

El sistema debe obligar automáticamente a que todos los usuarios cambien sus palabras claves al menos una vez cada treinta (30) días.

A menos que se tenga un permiso especial concedido por el administrador del sistema, el sistema no debe permitir que ningún usuario maneje simultáneamente sesiones

múltiples cuando esté en línea.

El sistema debe controlar el tiempo de inactividad del usuario y desactivar la sesión automáticamente.

Los usuarios no deben abandonar su lugar o estación de trabajo sin haber realizado log-out o haber cerrado la sesión.

A todos los usuarios se les debe revocar los privilegios automáticamente cuando no han tenido actividad durante un periodo determinado.