**ASOCIACION CIVIL MAGNUM CITY CLUB**

**Informe de Revisión Especial sobre**

**Procedimientos Previamente Convenidos**

**Diagnóstico Organizacional**

**Evaluación de Controles Generales Tecnológicos**

**2013**

**Evaluación de Controles Generales Tecnológicos**
**en ASOCIACION CIVIL MAGNUM CITY CLUB.**
**Revisión al 31 de julio de 2013.**

**A la Junta Directiva**
**Atención: Econ. Minerva Valleta**

La revisión de Controles Generales en el ambiente tecnológico de la **ASOCIACIÓN CIVIL MAGNUM CITY CLUB**, forma parte integral de la realización del diagnóstico operativo administrativo de los ciclos críticos que componen las actividades administrativas del club al 31 de julio de 2013. Nuestros procedimientos fueron diseñados principalmente para permitirnos evaluar los procesos sensibles y las acciones emprendidas por la Asociación para garantizar la integridad, consistencia y confidencialidad de la información, por lo que muchos de los aspectos evaluados, se basan en las mejores prácticas establecidas en estándares como CobiT (Objetivos de Control de tecnología de Información) y la Norma ISO 27001 y 27002 de Seguridad de la Información, entre otros estándares de Tecnología de Información.

El alcance de nuestra revisión no puede identificar todas las debilidades que pudiesen existir en los sistemas y procedimientos relacionados con los sistemas de información en la **ASOCIACIÓN CIVIL MAGNUM CITY CLUB.**

Las recomendaciones y observaciones en el área informática de la **ASOCIACIÓN CIVIL MAGNUM CITY CLUB**, relacionadas en las páginas siguientes, fueron discutidas con las personas responsables del Departamento de Informática. Este informe ha sido preparado para el uso exclusivo de la Gerencia de **ASOCIACIÓN CIVIL MAGNUM CITY CLUB** y no debe ser usado para ningún otro propósito. Agradecemos la colaboración prestada por el personal de la Institución, durante la ejecución de nuestro trabajo.

**LÓPEZ NIÑO & ASOCIADOS**

Fanny Mora
CPC No. 43.196

Caracas Venezuela, 22 de Octubre de 2013

## OBJETIVO Y ALCANCE DEL TRABAJO

El tipo de revisión empleada para evaluar la estructura de Controles Generales de Tecnología de Información en la **A.C. MAGNUM CITY CLUB,** persiguen comprobar el desempeño de la Organización en cuanto a los procedimientos de control implementados para garantizar la integridad, consistencia y confidencialidad de la información. Esta auditoría fue orientada al seguimiento de los procesos y a las acciones emprendidas por los responsables de los sistemas de información de la Organización, para dar cumplimiento a los aspectos de control estipulados en estándares como CobiT (Objetivos de Control de tecnología de Información) y la Norma ISO 27001 y 27002 de Seguridad de la Información, con el fin de generar las recomendaciones correspondientes que coadyuven a minimizar las brechas entre los riesgos de negocio, las necesidades de control y aspectos técnicos orientados a asegurar la seguridad y la eficiencia en los diferentes servicios prestados a los Asociados de la **A.C. MAGNUM CITY CLUB**.

## DETALLE DE OPORTUNIDADES DE MEJORAS

### 1. PLANEACIÓN ESTRATÉGICA Y ORGANIZACIÓN DE LOS RECURSOS DE INFORMACIÓN

### 1.1 Administración y Control de Proyectos

La Coordinación de Informática no dispone de herramientas ni metodología para la administración y control de Proyectos. Adicionalmente no disponen de un portafolio de proyectos tecnológicos correspondiente al periodo 2012-2013.

**Riesgos Identificados**

- Posibilidad que no se identifique oportunamente desviaciones en el cumplimiento de tareas de los proyectos, así como, no se apliquen los correctivos que correspondan, lo cual, podría incidir de forma negativa en el logro de las metas y actividades de la Gerencia de Tecnológica y esta situación podría conducir al incumplimiento de metas del negocio.
- Incremento en los recursos financieros asociados a los proyectos, debido al incumplimiento del tiempo y actividades.

**Recomendaciones**

- La Coordinación de Informática debe evaluar la posibilidad de implementar una Metodología de Control de Proyectos, a fin de que se establezcan los lineamientos por los cuales debe regirse la Gerencia de A.C. MAGNUM CITY CLUB para la administración y control de proyectos tecnológicos.
- Incluir en el portafolio general de proyectos aspectos que detalle: descripción, estado, responsables, fecha de inicio, fecha de finalización, porcentaje (%) de avance, estado activo, clasificación de proyectos a corto, mediano o largo plazo.
- La Coordinación de Informática debe preparar un Plan de Tecnología y debe ser documentado para su aprobación por la Junta Directiva de A.C. MAGNUM CITY CLUB, lo cual permitirá una supervisión continúa. De esta manera cumple con los controle mínimos que deben aplicarse para el logro de las metas y actividades del área tecnológica.
- Apoyarse temporalmente en herramientas semiautomatizadas o desarrolladas sobre software libre para la administración y control de proyectos.

## 2. MANTENIMIENTO E IMPLANTACIÓN DE LOS SISTEMAS DE INFORMACIÓN

### 2.1 Observaciones técnicas sobre el sistema de Control de Socios

Conocimos que existe un sistema utilizado para el Control de los Socios, el cual fue desarrollado en el Club. Este sistema de información fue desarrollado con una herramienta de programación llamada Visual Basic Versión 6.0 y sus tablas de datos son administradas por otra herramienta denominada SQL 2000.

Destacamos que el soporte estándar para Microsoft Visual Basic 6.0 finalizó el 31 de marzo de 2005, y se extendido formalmente hasta marzo de 2008, por lo cual, esta herramienta de programación, no se ajusta a las nuevas tecnologías en lo que refieres los aspectos técnicos a nivel de programación.

**Riesgos Identificados**

- La información de las tablas de datos, puede ajustarse o modificarse con bastante facilidad, utilizando procedimientos alternativos.
- La confidencialidad de la información, puede verse afectada.

**Recomendaciones**

Evaluar la posibilidad de desarrollar un sistema de información que técnicamente garantice confidencialidad, consistencia e integridad de datos y usuarios.

### 2.2 Actualización de Diccionario de Datos en los sistemas de Información

Conocimos que el diccionario de datos del Sistema "Control de Socios", no se encuentra disponibles en su totalidad y algunas de sus tablas se encuentran desactualizadas.

**Riesgos Identificados**

Un área de Desarrollo de Sistemas que no disponga de diccionarios de datos actualizados, trae consigo lo siguiente:

- Inversión de tiempo mayor en un desarrollador de sistemas que no conozca la definición de las tablas, su estructura y otros aspectos técnicos necesarios para su mantenimiento.
- Dependencia con analista desarrollador, quien conoce las tablas, campos que tiene cada una de ellas y el tipo de relación que existe entre ellas.

**Recomendaciones**

- Inventariar la totalidad de tablas existentes en el sistema "Control de Socios", identificando así todas las tablas relacionadas en los diferentes módulos del sistema, sus campos, tipo de campo y características particulares.
- Asegurar la creación y la continua actualización de un diccionario de datos corporativo que incorpore las reglas de sintaxis de datos a ser aplicados en la compañía.
- Planificar las recomendaciones anteriores en un proyecto con recursos dedicados únicamente a esa actividad con miras a lograr el objetivo planteado.

## 3. OPERACIONES DE LOS SISTEMAS DE INFORMACIÓN

### 3.1 No se encuentran documentadas las políticas y procedimientos relacionados con la ejecución de Respaldos.

En nuestro levantamiento de información, conocimos que la Coordinación de Sistemas de A.C. MAGNUM CITY CLUB, ejecuta diversos mecanismos relacionados con el proceso de respaldo y resguardo de la información, sin embargo, no existe un documento formal que logre ser considerado como un Manual de Políticas de Respaldo, el cual entre otros aspectos debe incluir:

3.1.1. Documentación sobre procedimientos para validar calidad de los respaldos realizados.

3.1.2. Procesos o tareas no incluidas en la documentación del proceso de respaldo:

- Clasificación de la información respaldada.
- Acciones tomadas en caso de fallos en el proceso de respaldo.
- Existencia de un registro cronológico y trimestral de los procesos ejecutados en el Centro de Procesamiento de Datos, que permitan el monitoreo y evaluación oportuna de todos los eventos relacionados.
- Niveles de escalamiento en caso de eventos importantes durante el proceso.
- Ejecución de pruebas a los dispositivos de respaldo utilizados.
- Procesos de simulacros de recuperación de información.

### 3.2 Ausencia de un esquema duplicado de Respaldos y resguardo externo de datos.

En la revisión efectuada al esquema de respaldo aplicado en A.C. MAGNUM CITY CLUB, identificamos procedimientos de ejecución y almacenamiento con una frecuencia irregular, cuyos dispositivos de almacenamiento son resguardados, sin embargo, no se contempla la ejecución por duplicado de los respaldos para ser resguardado fuera del Club. Esta situación es contraria a lo establecido en las mejores prácticas en el uso de los sistemas de información, como CobiT (Objetivos de Control de tecnología de Información) y la Norma ISO 27001 y 27002 de Seguridad de la Información, entre otros estándares de Tecnología de Información.

**Riesgos Generales Identificados en el Proceso de Respaldo**

- En caso de una contingencia o evento mayor en el edificio Sede donde se encuentran los respaldos internos, no se dispone con otra fuente confiable de respaldos, por lo que no se garantiza la inmediata continuidad del negocio.
- Al no existir Normas en torno a la restauración de los respaldos, podría afectarla disponibilidad inmediata de la información resguardada.
- En caso de una contingencia o evento mayor, al no realizarse pruebas certificadas de recuperación de datos, la confiabilidad de los respaldos estaría en entredicho, por lo que no se garantiza la inmediata continuidad del negocio.

**Recomendaciones Generales**

- Documentar las Políticas, Normas y Procedimientos para el área de operaciones, que incluya formalizar procedimientos para la ejecución, restauración y resguardo de la información respaldada.
- Incluir procedimientos de pruebas periódicas de los dispositivos de respaldo externos, la creación de documentos y/o soportes que avalen las pruebas realizadas a los dispositivos de almacenamiento e información respaldada.
- Determinar con exactitud en el Manual de Normas y procedimientos el tiempo que será conservada la información respaldada.

- Otros aspectos que deben ser documentados:
  - Clasificación de la información respaldada.
  - Acciones tomadas en caso de fallos en el proceso de respaldo.
  - Niveles de escalamiento en caso de eventos importantes durante el proceso.
  - Ejecución de pruebas a los dispositivos de respaldo utilizados.
  - Procesos de simulacros de recuperación de información.
  - Identificar los servidores a los que se les debe realizar el respaldo de la información.

## 4. REDES E INFRAESTRUCTURA DE TELECOMUNICACIONES

### 4.1 No hay evidencias del monitoreo sobre las redes y su rendimiento.

Aunque el Departamento de Informática monitorea el comportamiento de la red y sus aplicaciones, se apoya en la herramientas propias del sistema operativo ya que los analistas no disponen con una herramientas automatizada para el monitoreo de las operaciones a nivel de red y aplicaciones.

**Riesgos Identificados**

Complejidad en el seguimiento de accesos no autorizados al sistema y ejecución de transacciones críticas, así como, rápida y efectiva identificación de los responsables en caso de cualquier eventualidad ocurrida. Por otra parte, impide visualizar y posiblemente corregir los errores ocurridos durante el funcionamiento del sistema de forma oportuna.

**Recomendaciones**

- Evaluar la posibilidad de adquirir una herramienta que apoye el proceso de monitoreo de eventos en la plataforma, que incluya el desempeño de los servidores y aspectos de seguridad de acceso, para casos de ataques de intrusos.
- Definir indicadores operativos para el análisis de los registros generados, los cuales servirán de apoyo a los informes estadísticos, que incluya todos los componentes (ruteadores (routers), interruptores (switches), firewalls, segmentación de redes, administración del desempeño, acceso remoto, etc.)

### 4.2 Documentación técnica asociada a la Infraestructura de Telecomunicaciones

No existe documentación técnica del esquema de cableado y conectividad en la infraestructura de telecomunicaciones, lo cual incluye lo siguiente:

- Documentación descriptiva de los elementos de cableado.
- Planos de trayectoria del cableado.
- No hay certeza que el sistema de cableado esté debidamente certificado conforme en lo establecido por la norma ANSI/EIA/TIA-606.

**Riesgos Identificados:**

- Es posible que la administración de todo el sistema de cableado de telecomunicaciones, tenga mayor complejidad y la inversión de tiempo sería mayor.
- El conocimiento de los elementos de cableado es muy escaso por lo que es factible que cualquier rediseño del cableado seria complejo, lo cual haría más complejo el rastreo de líneas, medición de transmisión, etc.
- Es posible que el sistema de cableado se pudiese ver comprometido, debido a la falta de certificación del mismo, al no tener conocimiento de vida útil, parámetros eléctricos adecuados de acuerdo a las normas, entre otras.

**Recomendaciones:**

- Evaluar la posibilidad de marcar el sistema de cableado con el código de color que corresponda, según se encuentra definido en la norma ANSI/EIA/TIA-606.
- Aplicar lo establecido en las mejores prácticas establecidas en estándares como CobiT (Objetivos de Control de tecnología de Información) y la Norma ISO 27001 y 2 002 de Seguridad de la Información, entre otros estándares de Tecnología de Información relacionado con el rastreo de líneas y circuito de comunicación, medición de la transmisión de telecomunicaciones y analizar los registros de paquetes que viajan en la red.
- Evaluar la posibilidad de adquirir herramientas de monitoreo que permitan obtener la información mencionada en el punto anterior, si es necesario.

## 5. PLAN DE CONTINGENCIA TECNOLÓGICA

### 5.1 Documentación informal de los Planes de Contingencia y ausencia de un Plan de Continuidad de Negocios

Actualmente la Coordinación de Informática, aunque posee conocimientos que pueden ser aplicadas en casos de alguna contingencia, no existe ningún tipo de documentación formal que pueda ser considerada como un Plan de Contingencia.

De igual manera, conocimos que no existe un Plan de Continuidad de Negocios, que permita asegurar la continuidad operativa y financiera, satisfacción de los clientes y productividad a pesar de una catástrofe.

Es importante destacar que mientras en un plan de contingencia se concentran esfuerzos en la recuperación de eventos únicos que producen una interrupción prolongada del servicio, el plan de continuidad se ejecuta permanentemente a través de la administración de riesgos tanto en la información como en la operación.

**Riesgos Identificados**

- Dependiendo del tipo de contingencia, existe la posibilidad de paralización parcial o total de las operaciones debido a la carencia de un documento que establezca las estrategias para garantizar su recuperación ante cualquier contingencia. Cuando las líneas de comunicación en una empresa se interrumpen, desconectando los sistemas, o cuando se daña un disco duro, o se pierde el acceso al centro de cómputo, se corre el riesgo de grandes pérdidas.
- No se podría reaccionar adecuadamente a una falta en un proceso crítico.

**Recomendaciones**

- Desarrollar un proyecto que incluya la identificación de los factores críticos, el establecimiento de los equipos de trabajo y alternativas de solución de la contingencia, una prueba real del mismo plan, capacitación de las personas involucradas y una constante actualización.
- Considerando que el plan de continuidad es costoso, se debe evaluar para los sistemas de alta criticidad, implementar un plan de continuidad, para otros, bastará con un plan de contingencia.

Los planes de contingencia y Continuidad del Negocio tienden a ser confundidos, a continuación presentamos un esquema donde se establecen diferencias:

| Plan de Contingencia | Plan de Continuidad de Negocios |
|---|---|
| • Tiene como beneficio para el Centro de Especialidades Médicas garantizar la recuperación de servicios que están desmejorados por la falla, en un período de entre 12 y 72 horas. Un plan de contingencia se refleja en un documento que especifican las tareas que hay que hacer antes, durante y después de la contingencia, además de los responsables de cada acción.<br>• Se restablece el servicio de los procesos críticos a la mayor brevedad. | • Se basa sobre las tecnologías emergentes (como unidades de discos para redes, SAN, y cintas para copias de respaldo de altísima velocidad), y la excelencia operativa del centro de cómputo.<br>• No hay interrupción del servicio. |
| Debe quedar claro que un plan de continuidad no es excluyente de un plan de contingencia, sino más bien que el segundo está dentro del primero. Un plan de continuidad para el negocio debe incluir: un plan de recuperación de desastres, el cual especifica la estrategia de un negocio para implementar procedimientos después de una falla; un plan de reanudación que especifica los medios para mantener los servicios críticos en la ubicación de la crisis; un plan de recuperación que especifica los medios para recuperar las funciones del negocio en una ubicación alterna; y un plan de contingencia que especifica los medios para manejar eventos externos que puedan tener serio impacto en la organización. | |

## 6. SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

### 6.1 Ausencia de un Manual con las Políticas, Normas y Procedimientos de Seguridad de la información.

Conocimos que en A.C. MAGNUM CITY CLUB poseen una serie de lineamientos relacionados con la seguridad de los activos de información, sin embargo, algunos no se encuentran documentados y otros no se encuentran formalizados y aprobados en un único documento que contenga estas normativas.

En tal sentido, no existen lineamientos entre otros, relacionados con:

6.1.1 Destrucción de reportes, listados u otros medios de información provistos por sistemas electrónicos, no vigentes o en desuso.
6.1.2 Políticas de respaldos y Monitoreo de logs en los sistemas de información críticos de A.C. MAGNUM CITY CLUB.
6.1.3 Procedimientos para reportar "vulnerabilidades de seguridad" en la plataforma tecnológica.
6.1.4 Uso de Internet y correo electrónico.
6.1.5 Monitorear los procesos de control de cambio y pases a producción de los sistemas y aplicaciones productivas.
6.1.6 Realizar el control y seguimiento continuo a los accesos efectuados a los activos de información.

**Riesgos generales identificados**

- La ausencia formal de un responsable de seguridad de datos, podría propiciar debilidades para aplicar y asegurar el cumplimiento de las políticas de seguridad de la información definidas, monitorear los procesos de control de cambio y pases a producción de los sistemas y aplicaciones productivas, realizar el control y seguimiento continuo a los accesos efectuados a los activos de información, entre otras.
- Posibilidad de fuga de información y divulgación de la misma al momento de destrucción de reportes o listados en desuso.
- Es factible no conocer oportunamente accesos no autorizados al sistema y ejecución de transacciones críticas, que no se identifique oportunamente los responsables en
- caso de cualquier eventualidad ocurrida, así como podría impedir visualizar y posiblemente corregir los errores ocurridos durante el funcionamiento del sistema. Imposibilidad de mantener activos los registros o pistas de auditoría generadas por las aplicaciones y sistemas de misión crítica.

**Recomendaciones**

- Proponer la creación del Manual de Funciones y Cargos correspondiente al área de Seguridad de Datos, para su pronta formalización y aprobación.
- Validar que el manual de seguridad de información propuesto, contenga lo siguiente: Procedimientos para el resguardo de los listados y documentación de datos, programas y sistemas, procedimientos para destrucción de material sensitivo, procedimientos de monitoreo de logs de los diversos sistemas de información utilizados en A.C. MAGNUM CITY CLUB., procedimientos para reportar cualquier tipo de vulnerabilidades, velar por el cumplimiento de las políticas de seguridad de los activos de información entre otros.
- Establecer lineamientos formales para el envío y recepción de correos electrónicos, clasificación de la información que debe ser transmitida con el uso de la cuenta del correo electrónico.

### 6.2 Valores definidos en las Directivas de Seguridad de Windows 2008 Server.

En el transcurso de nuestra auditoría solicitamos información técnica del sistema operativo del servidor configurado como Primary Domain Controller y conocimos que las diversas directivas de seguridad, se encuentran en sus definiciones estándar, por lo cual, no ajustan a las mejores prácticas y/o recomendaciones del proveedor. Estas directivas son las siguientes:

- Registro de Sucesos
- Directivas de Contraseñas
- Directiva de Bloqueo de Cuentas
- Directiva de Kerberos
- Opciones de Seguridad

Los valores definidos en cada una de estas directivas que no se ajustan a las mejores prácticas son los siguientes:

| Registro de Sucesos | | |
|---|---|---|
| Parámetro | Valor Actual | Recomendación |
| Evitar que el grupo de invitados locales tenga acceso al registro de aplicaciones | No está definido | Habilitado |
| Evitar que el grupo de invitados locales tenga acceso al registro de seguridad | No está definido | Habilitado |
| Evitar que el grupo de invitados locales tenga acceso al registro del sistema | No está definido | Habilitado |

**Riesgos:**
Un atacante que ha conseguido iniciar sesión en un equipo con privilegios de invitado puede obtener información importante sobre el sistema consultando los registros de sucesos y seguir realizando más ataques.

| Directiva de Contraseñas | | |
|---|---|---|
| Parámetro | Valor Actual | Recomendación |
| Forzar el historial de contraseñas | No está definido | 12 |
| Las contraseñas deben cumplir los requerimientos de complejidad . | No está definido | Habilitar |
| Vigencia máxima de la contraseña | No está definida | 30 - 45 días |
| Vigencia mínima de la contraseña | No está definida | 0 |

**Riesgos:**
- Reutilización de contraseñas con poco o ningún nivel de seguridad.
- Apropiación indebida de claves de otros usuarios sin consentimiento del responsable.
- Claves de fácil identificación por parte de usuarios externos con intenciones de acceder a la red y datos

| Directiva de Bloqueo de Cuentas | | |
|---|---|---|
| Parámetro | Valor Actual | Recomendación |
| Duración del bloqueo de cuenta | 20 minutos | 30 minutos |
| Restablecer la cuenta de bloqueos después de: | 20 minutos | 30 minutos |

**Riesgos:**
Un ataque de denegación de servicio (DoS) se puede crear si un atacante altera el Umbral de bloqueos de la cuenta e intenta iniciar sesión en una cuenta de forma repetida. Si se configura el Umbral de bloqueos de la cuenta, la cuenta se bloqueará tras el número de intentos erróneos especificado.

| Directiva de Kerberos | | |
|---|---|---|
| Parámetro | Valor Actual | Recomendación |
| Edad máxima de renovación de tíquets de usuario | No está definida | 10.080 |
| Forzar restricciones de inicio de sesión de usuario | No está definido | Habilitar |
| Tolerancia máxima para la sincronización de los relojes de los equipos | No está definida | 5 minutos |
| Vigencia máxima del vale de servicio | No está definida | 600 minutos |
| Vigencia máxima del vale de servicio | No está definida | 600 minutos |

**Riesgos:**
- Se podrán conceder vales de sesión a los usuarios para servicios que no tienen derecho a utilizar.
- Los usuarios pueden obtener acceso a los recursos de red fuera de las horas de inicio de sesión, o que los usuarios cuyas cuentas se hayan deshabilitado continúen teniendo acceso a los servicios de red por medio de vales de servicio válidos emitidos antes de que se deshabilitara la cuenta.
- Para evitar "ataques de reproducción", Kerberos utiliza marcas de tiempo como parte de su definición de protocolo. A fin de que las marcas de tiempo funcionen adecuadamente, los relojes del cliente y del controlador de dominio necesitarán estar sincronizados al máximo.

| Opciones de Seguridad | | |
|---|---|---|
| Parámetro | Valor Actual | Recomendación |
| Acceso de red: | | |
| Permitir traducción SID/nombre anónima | No está definido | Habilitar |
| Deja que los permisos de Todos se apliquen a los usuarios anónimos | No está definido | Habilitar |
| Restringir acceso anónimo a canalizaciones con nombre y recursos compartidos | No está definido | Habilitar |

**Riesgos:**
- Un usuario podrá utilizar el SID conocido del administrador para obtener el nombre real del administrador integrado, incluso si se ha cambiado el nombre de la cuenta. Esa persona podría entonces utilizar el nombre de cuenta para iniciar un ataque de averiguación de contraseña.
- Un usuario no autorizado podría obtener de forma anónima una lista de os nombres de las cuentas y los recursos compartidos y utilizar dicha información para intentar averiguar contraseñas o realizar ataques de ingeniería social.

| Opciones de Seguridad | | |
|---|---|---|
| Parámetro | Valor Actual | Recomendación |
| Acceso a redes: | | |
| Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM | No está definido | Habilitar |
| Acceso a redes: no permitir el almacenamiento de credenciales o .NET Passports para la autenticación del dominio | No está definido | Habilitar |
| Acceso de red: modelo de seguridad y recursos compartidos para cuentas locales | No está definido | Clásico: usuarios locales autenticados como ellos mismos |
| Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM | No está definido | Habilitar |

**Riesgos:**

- Un usuario no autorizado puede obtener de forma anónima una lista con los nombres de cuentas y utilizar dicha información para intentar averiguar contraseñas o realizar ataques de ingeniería social.
- Cuando inicie sesión en el equipo, un usuario podrá tener acceso a las contraseñas almacenadas en caché de esta forma. Puede resultar obvio, pero el problema surge cuando un usuario ejecuta sin saberlo un código hostil que lee las contraseñas y las reenvía a otro usuario no autorizado.
- Con el modelo de sólo invitado, cualquier usuario que pueda tener acceso a su equipo a través de la red lo hace con privilegios de invitado. Esto significa que probablemente no podrán escribir en esos recursos compartidos. Mientras que así se aumenta la seguridad, imposibilita a los usuarios autorizados obtener acceso a recursos compartidos en estos sistemas.

| Inicio de sesión interactivo: | | |
|---|---|---|
| Núm. de inicios de sesión previos en la caché (en caso que el controlador de dominio no esté disponible) | No está definido | 0 |
| Pedir al usuario cambiar la contraseña antes de que caduque | No está definido | 14 días |
| Requerir la autenticación del controlador de dominio para desbloquear el equipo | No está definido | Habilitar |
| Mostrar información de usuario cuando se bloquee la sesión | No está definido | Deshabilitado |

**Riesgos:**

- Deberá avisarse a los usuarios de que su contraseña va a caducar o, de lo contrario, es probable que el sistema se bloquee de forma inesperada.
- Al emplear credenciales almacenadas en caché, cualquier cambio realizado recientemente en la cuenta (como asignaciones de derechos de usuario, bloqueo de cuentas o que la cuenta esté deshabilitada) no se tendrá en cuenta o no se aplicará hasta que el proceso de autenticación haya finalizado.

| Inicio de sesión interactivo: | | |
|---|---|---|
| No mostrar el último nombre de usuario | No está definido | Habilitar |
| Texto del mensaje para los usuarios que intentan iniciar una sesión | No está definido | Ver 1 |
| **(1)** Establezca Texto del mensaje para los usuarios que intentan iniciar una sesión en el siguiente valor de mensaje:<br>El acceso a este sistema está restringido a usuarios autorizados. Todo individuo que intente tener acceso a él sin autorización será perseguido por la ley. Si no tiene autorización, debe terminar el acceso de forma inmediata. Si hace clic en Aceptar, significa que acepta la información anterior. | | |
| Título del mensaje para los usuarios que intentan iniciar una sesión | No está definido | Ver 2 |
| **(2)** Establezca **Título del mensaje para los usuarios que intentan iniciar una sesión** en el siguiente valor de mensaje:<br>SE CONSIDERA DELITO CONTINUAR SIN LA AUTORIZACIÓN ADECUADA. | | |

**Riesgos:**

- Un atacante con acceso a la consola (p. ej., alguien con acceso físico o que puede conectarse al servidor por medio de los Servicios de Terminal Server) podría ver el nombre del último usuario que inició sesión en el servidor. De este modo, podría intentar iniciar sesión en el servidor mediante un ataque de averiguación de contraseña.
- Si no se utilizan mensajes de advertencia, la organización quedará vulnerable legalmente ante los intrusos que penetren en la red de forma ilegal

| Opciones de Seguridad | | |
|---|---|---|
| Parámetro | Valor Actual | Recomendación |
| **Cuentas:** | | |
| limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar la consola. | No está definido. | Habilitar |
| **Auditoría:** | | |
| Auditar el acceso de objetos globales del sistema | No está definido | Habilitar |
| Apagar el sistema de inmediato si no puede registrar auditorías de seguridad. | No está definido | Habilitar |
| **Dispositivos:** | | |
| Permitir formatear y expulsar medios extraíbles | No está definido. | Administrador |
| Impedir que los usuarios instalen controladores de impresora | No está definido. | Habilitar |
| Restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente | No está definido. | Habilitar |
| Restringir el acceso a la unidad de disquete sólo al usuario con sesión iniciada localmente | No está definido. | Habilitar |

**Riesgos:**

- Las contraseñas en blanco constituyen una seria amenaza para la seguridad del equipo y, por lo tanto, deberían prohibirse tanto con medidas técnicas pertinentes como con directivas corporativas.
- Sí no se protege un objeto con nombre Visible globalmente del modo adecuado, podrá ser centro de un ataque por parte de un programa malintencionado que sepa su nombre.
- No se podrá disponer de pruebas esenciales o información clave relativa a la solución de problemas para realizar una revisión tras haberse producido una incidencia de seguridad.
- Los usuarios podrían mover discos extraíbles a otro equipo donde disfruten de privilegios administrativos para, de este modo, poder tomar posesión de cualquier archivo, otorgarse control total sobre él y verlo o cambiarlo.

| Opciones de Seguridad | | |
|---|---|---|
| Parámetro | Valor Actual | Recomendación |
| **Seguridad de red:** | | |
| No almacenar valor de hash de LAN Manager en el próximo cambio de contraseña | No está definido | Habilitar |
| Forzar el cierre de sesión cuando expire la hora de inicio de sesión | No está definido | Habilitar |

**Riesgos:**

- Al atacar el archivo SAM, los atacantes pueden obtener acceso potencialmente a los hashes de nombre de usuario y contraseña. Los atacantes pueden utilizar una herramienta de averiguación de contraseñas para determinar la contraseña.
- Si se deshabilita este valor, un usuario puede permanecer conectado al sistema fuera de sus horas de inicio de sesión permitidas.

| Opciones de Seguridad | | |
|---|---|---|
| Parámetro | Valor Actual | Recomendación |
| **Objetos de sistema:** | | |
| Propietario predeterminado para objetos creados por miembros del grupo de administradores | No está definido | Creador de Objetos |
| Requerir diferenciación de mayúsculas y minúsculas para subsistemas no basados en Windows | No está definido | Habilitar |
| Reforzar los permisos predeterminados de los objetos internos del sistema (p.e. vínculos simbólicos) | No está definido | Habilitar |

**Riesgos:**

- Al establecer este valor de configuración, el grupo Administradores impedirá que se responsabilice a los individuos por crear objetos de sistema nuevos.
- Dado que Windows no hace distinción de mayúsculas y minúsculas, pero el subsistema POSIX sí, no aplicar esta configuración hace que sea posible que un usuario de ese subsistema cree un archivo con el mismo nombre que otro archivo utilizando mayúsculas y minúsculas en el nombre. A la larga, esto podría confundir a los usuarios cuando intentaran obtener acceso a estos archivos con herramientas normales de Win32.

| Opciones de Seguridad | | |
|---|---|---|
| Parámetro | Valor Actual | Recomendación |
| Otros: | | |
| Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión | No está definido | 15 minutos |
| Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite) | No está definido | Habilitar |
| Apagado: permitir apagar el sistema sin tener que iniciar sesión | No está definido | Deshabilitado |

**Riesgos:**

- Cada sesión SMB consume recursos del servidor, de manera que si se establecen varias sesiones nulas, el servidor puede funcionar más lento o incluso bloquearse. Un atacante puede establecer sesiones SMB de forma repetida hasta conseguir que el servidor deje de responder y, en consecuencia, los servicios SMB serán más lentos o no responderán.
- Los usuarios que tienen acceso a la consola localmente pueden apagar el sistema. Los atacantes o usuarios malintencionados podrían conectarse al servidor mediante Servicios de Terminal Server y apagarlo o reiniciarlo sin tener que identificarse.

## Recomendaciones

- Evaluar las opciones correspondientes a las políticas de auditorías (Audit Policy), los parámetros de seguridad (Security Options) y los privilegios a los usuarios (User Rights Assignment) y active las que considere necesarias de acuerdo con los riesgos y las amenazas en la plataforma tecnológica del Centro Médico.
- Definir el tamaño adecuado de los registros según la criticidad de los datos, la frecuencia de revisión de los registros y el espacio disponible en el disco de los servidores. Una vez se alcance el tamaño definido, se debe realizar un respaldo de los mismos.
- Restringir el acceso a los registros a personas autorizadas.
- Examinar periódicamente los eventos o los incidentes grabados en los registros provistos por el sistema operativo del servidor principal para conocer las posibles violaciones de seguridad que pudieran ocurrir en los sistemas de información de la red y tomar prontamente las medidas preventivas y correctivas necesarias.
- Revisar periódicamente los eventos registrados en el servidor principal y de ser necesario, tomar de inmediato las medidas preventivas y correctivas.

Agradecemos la colaboración recibida de parte del personal de la **ASOCIACION CIVIL MAGNUM CITY CLUB** durante el desarrollo de nuestra participación en este trabajo.

Quedamos en la disposición de aclarar cualquier duda existente sobre los puntos planteados en el presente informe.