UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

FACULTAD DE INGENIERÍAS

CARRERA DE INGENIERÍA DE SISTEMAS

TESIS DE GRADO

PREVIA A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO DE SISTEMAS

TÍTULO:

"ANÁLISIS Y SOLUCIÓN DE LAS VULNERABILIDADES DE LA SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN DE UN MEDIO DE COMUNICACIÓN AUDIO-VISUAL"

AUTORES:

Gabriela Arias Buenaño

Nelson Merizalde Almeida

Natasha Noriega García

DIRECTOR:

Ing. Dario Huilcapi Subia

Guayaquil, Octubre 2013

AGRADECIMIENTO

Primordialmente agradecemos a la Universidad Politécnica Salesiana puesto que nos brindó conocimientos y nos ayudó en el desarrollo de nuestro proyecto de grado y a la elaboración final de este.

A los profesores que nos brindaron su sabiduría en varios campos del conocimiento ayudándonos así en varios aspectos que requerimos para el desarrollo de nuestro proyecto y vida profesional.

Gabriela Arias Buenaño

AGRADECIMIENTO

Quiero agradecer a mis padres que con su apoyo, confianza y motivación he logrado terminar esta etapa de mi vida de manera exitosa; llegar hasta aquí no ha sido fácil, se presentaron dificultades en el camino pero gracias a que fueron mi soporte pude superar muchos obstáculos.

De igual manera agradezco a todos los profesores que formaron parte de esta etapa, unos fueron solo docentes y otros se convirtieron en verdaderos guías e incluso amigos, agradezco a cada uno de ellos por haber compartido su conocimiento, experiencia y por brindarme la oportunidad de aprender de ellos.

Por último y no menos importante a mis compañeras de clase y amigas Gabriela y Natasha que formaron parte importante de esta etapa.

Nelson Merizalde Almeida

AGRADECIMIENTO

Agradezco a Dios quien ha sido mi pilar fundamental en el desempeño de mi vida profesional brindándome la fuerza para atravesar los obstáculos sin perder nunca la dignidad, ni desfallecer en el intento.

También agradezco a los profesores y a la Universidad Politécnica Salesiana por brindarme la oportunidad de aprender.

Natasha Noriega García

DEDICATORIA

Principalmente dedico este trabajo a mis hermanos que son mi pilar fundamental de vida y esfuerzo para cada día salir adelante, mis padres Hernán y Betty que juntos y por separado han sabido forjar en mí buenos principios brindándome apoyo y fortaleza en el desarrollo de mi carrera.

Dedico este proyecto a Dios que nos brinda sabiduría, amor y paciencia, nos ayuda en los momentos más difíciles dándonos valores y perseverancia que nos fortalecen no sólo como trabajo de grupo, sino también como personas.

A mis abuelitos Elsa y Humberto que me criaron y están a mi lado incondicionalmente.

A mis amigos Natasha y Nelson, sin ustedes mi vida universitaria no hubiese tenido ese apoyo grupal con el que siempre contamos para salir victoriosos de cada batalla (semestres).

Gabriela Arias Buenaño

DEDICATORIA

Dedico este trabajo a todas las personas que han sido parte de mi formación universitaria, profesores, compañeros, amigos y familiares. Esta meta alcanzada es dedicada principalmente a mis padres que son quienes me han brindado apoyo incondicional durante cada etapa de mi vida, dándome la oportunidad de crecer como persona y como profesional.

Nelson Merizalde Almeida

DEDICATORIA

A mis padres Guillermina y Mario quienes me han apoyado con sus consejos, compresión y amor. Ayudándome con los recursos necesarios para desempeñarme correctamente en mis estudios.

A mis hermanos Jessica y Marcelo por estar siempre presentes en los momentos significativos de mi vida, escuchándome y ayudándome en cualquier momento.

A mis compañeros Gabriela y Nelson por su amistad desde los inicios de nuestra vida universitaria y estar a mi lado hasta lograr esta meta.

Natasha Noriega García

DECLARACIÓN DE RESPONSABILIDAD

Nosotros Gabriela Arias Buenaño, Nelson Merizalde Almeida y Natasha Noriega García, declaramos que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

Guayaquil, Octubre del 2013

Gabriela Arias Buenaño

AUTOR

Nelson Merizalde Almeida

AUTOR

Natasha Noriega García

AUTOR

CERTIFICADO

Certifico que el presente trabajo fue realizado por los Sres. Gabriela Arias Buenaño, Nelson Merizalde Almeida y Natasha Noriega García, bajo mi supervisión.

Guayaquil, Octubre del 2013

Dario Huilcapi Subia

DIRECTOR DE TESIS

Integrantes: Gabriela Arias Buenaño
Nelson Merizalde Almeida
Natasha Noriega García

TESIS UPS-G: CARRERA DE INGENIERIA DE SISTEMAS

TEMA: "ANÁLISIS Y SOLUCIÓN DE LAS VULNERABILIDADES DE LA SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN DE UN MEDIO DE COMUNICACIÓN AUDIO-VISUAL"

RESUMEN

En este estudio se ha auditado, recomendado e implementado políticas generales de seguridad informática y seguridad de la información en la empresa, el objetivo ha sido poder manejar su sistema de gestión de la seguridad de la información siguiendo procedimientos estandarizados que permiten identificar y reducir a corto y mediano plazo los diferentes riesgos informáticos, así como incidentes que involucran a la información que pueden ser accidentales o provocados como alteraciones, accesos no autorizados, o en su defecto, fuga o pérdida de información de vital importancia para la continuidad del negocio. Mediante conversaciones con los miembros del departamento de tecnologías de información y una entrevista final al responsable del área, se pudo concluir que la mayoría de los riesgos identificados de seguridad informática y seguridad de la información en la empresa eran de nivel intermedio y críticos, esto representaba un alto riesgo para la empresa por estar comprometida su información y su infraestructura tecnológica debido a que carecían de varios controles de seguridad necesarios y también porque sus políticas generales de seguridad tenían múltiples falencias. Aplicando mejoras y recomendaciones basadas en varios dominios, objetivos de control y controles de la norma ISO 27002:2005 se logró reducir gradualmente los riesgos de nivel bajo, intermedios y críticos de seguridad informática y seguridad de la información identificados al inicio de este estudio.

PALABRAS CLAVES: Auditoría; estándar; ISO 27002:2005; políticas; seguridad; seguridad de la información; seguridad informática.

Members: Gabriela Arias Buenaño
Nelson Merizalde Almeida
Natasha Noriega García

UPS-G THESIS: SYSTEMS ENGINEERING CAREER

TOPIC: "ANALYSIS AND SOLUTION OF THE VULNERABILITIES OF COMPUTER SECURITY AND INFORMATION SECURITY FROM AN AUDIO-VISUAL COMMUNICATION MEDIUM"

ABSTRACT

This study had audited, recommended and implemented general policies of computer security and information security in the company, the goal has been to manage its system management of information security following standardized procedures to identify and reduce in the short and medium term different computer risks, as well as incidents involving the information that may be accidental or deliberate, such as alterations, unauthorized access, or otherwise, leak or loss of vital information for the business continuity. Through interviews to the members of the information technology department and a final survey to the area manager, it was concluded that most of the currently identified risks of computer security and information security in the company are intermediate and critics, this represented a high risk to the company by being committed its information and its technological infrastructure due to its lacked of necessary security controls and also because its general safety policies had multiple flaws. Applying improvements and recommendations based on multiple domains, control objectives and controls in the ISO 27002:2005 standard achieved gradually reduce risks of low, intermediate and critic level of computer security and information security, identified at the beginning of this study.

.

KEY WORDS: Audit; computer security; information security; ISO 27002:2005; policies; security; standard.

ÍNDICE INICIAL

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

En los últimos años, con los acelerados y grandes avances tecnológicos, los sistemas informáticos se han constituido en la herramienta más poderosa para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, los sistemas de información de las empresas que no solo manejan datos básicos del negocio sino que también la columna o estructura central de la organización.

La sociedad actual ha incrementado considerablemente la probabilidad y potencialidad de esas amenazas por causas tan diversas como el empleo de poderosas aplicaciones de procesos tecnológicos y el mal uso de las mismas, con el pasar del tiempo se han implementado nuevas técnicas de protección contra amenazas provenientes de diversas fuentes que pueden llevar a reflejar problemas en la logística del negocio o hasta pérdida de capital. Aunque cabe recalcar que la informática no gestiona propiamente la organización, sirve de soporte para los procesos de gestión y ayuda a la toma de decisiones. [1]

La informática de hoy está inmersa en la gestión integral de las empresas por lo tanto la seguridad es un elemento fundamental, los departamentos de sistemas de cada organización deben dar siempre prioridad a la seguridad de los sistemas de información. Existen actualmente normas y estándares informáticos los cuales garantizan integridad, disponibilidad y confidencialidad de los sistemas de información para así ofrecer calidad y transparencia en los procesos informáticos críticos de la organización. Los riesgos actuales que se presentan en los sistemas informáticos y el medio en el cual los empleados desarrollan sus cotidianas actividades profesionales traen como consecuencia un conjunto de amenazas informáticas permanentes. Una empresa puede tener el 80% o 100% de información crítica, sensible y confidencial en bases de datos, correos o documentos que sin un previo proceso de resguardo y cuidado pueden sufrir de alteraciones no autorizadas.[2]

[1] (Marité, 2010)
[2] (BSecure, 2010)

CAPÍTULO 1

1 DISEÑO DE LA INVESTIGACIÓN

1.1 Antecedentes de la investigación

La empresa sujeto de este estudio es un medio público de comunicación televisiva nacional, que lleva décadas informando y entreteniendo a la audiencia ecuatoriana con programación nacional y extranjera utilizando para su transmisión diaria una infraestructura tecnológica competitiva y de última generación.

Actualmente posee una infraestructura de red y comunicación dividida en la matriz localizada en la ciudad de Guayaquil y su sucursal en la ciudad de Quito, a través de enlaces de microondas y del anillo nacional de red de fibra óptica de Telconet.

El departamento de tecnologías de la información (TI) gestiona la seguridad de la información empleando métodos no estandarizados orientados al control de la fuga de información, administración de activos, actualización constante de los sistemas operativos y sus aplicaciones, directorios activos y monitoreo de flujo de navegación, para así llevar un mejor control de la seguridad informática y de la información dentro de la organización pero con falencias en la estructura, esquema y procedimientos de revisiones y aplicaciones para evitar las distintas vulnerabilidades informáticas.

Por motivos de seguridad la empresa solicitó no sea revelado su nombre ni información como direcciones de red tanto locales como públicas, nombres reales de los servidores y cualquier información sensible que pueda comprometer su seguridad e integridad, con esto se pretende proteger su infraestructura tecnológica de posibles ataques, por lo tanto hemos procedido a llamarla “GNN7 TV” en el desarrollo de la tesis, ya que el documento será de dominio público.

1.2 Problema de investigación

1.2.1 Planteamiento del problema

El departamento de tecnologías de la información (TI) en los últimos años ha implementado controles y mecanismos para la seguridad informática y seguridad de la información, pero como ya sabemos cada innovación trae aspectos positivos y negativos; en este caso la empresa "GNN7 TV" requiere una auditoría/consultoría informática ya que en su sistema de gestión de seguridad de la información (SGSI) existen falencias ya identificadas como controles mal implementados y una mala administración de la red, presentando pérdidas o fugas parciales de información de alta importancia para el negocio.

Al no ser corregidas las falencias mencionadas, la empresa GNN7 TV se verá afectada y comprometida de manera incremental con el pasar del tiempo en diferentes aspectos, por un lado su motor principal y del cual obtiene rentabilidad que es el sistema de transmisión no estará cien por cierto operativo y por ende provocará pérdidas económicas, por otra parte las áreas administrativas, financieras y gerenciales las cuales manejan información vital para la gestión del negocio estarán expuestas a robos informáticos o fuga de información, las falencias detectadas deben ser resueltas a través de diferentes mecanismos que ayuden a encontrar debilidades y vulnerabilidades en los actuales procesos informáticos de la organización. Tomaremos como base del proyecto varios de los controles especificados en la norma ISO/IEC 27002:2005 [3], esta norma está enfocada a establecer controles en todos los procesos informáticos que involucran información con el fin de optimizarlos, mejorar la seguridad de la red, controlar el acceso a la información y gestionar el uso de los recursos tecnológicos, a partir de esto se harán recomendaciones de buenas y mejores prácticas informáticas y se van a proponer soluciones a los diferentes aspectos de seguridad informática y seguridad de la información detectados en GNN7 TV. En caso de no ser viables las soluciones propuestas en este proyecto estas serán tomadas como alternativas a implementar en el futuro y así optimizar sus mecanismos de seguridad.

[3] ISO/IEC: Interntional Organization for Standarization / Internacional Electrotechnical Commission

1.2.2 Formulación del problema de investigación

Como producto del planteamiento del problema vamos a formular una pregunta que será el punto de partida de nuestra investigación

- ¿Cómo determinar que los procesos actuales de seguridad informática y de la información no son los adecuados para la organización?

1.2.3 Sistematización del problema de investigación

Para sistematizar el problema vamos a descomponer la pregunta planteada en la formulación del problema de tal manera que podamos segmentar nuestro estudio:

- ¿Por qué la gestión actual de la seguridad de la información que lleva acabo la empresa no es eficiente?
- ¿Por qué la no estandarización del SGSI provoca riesgos de seguridad?
- ¿Cuáles son los factores que inciden para que se presenten interrupciones y fallos en la infraestructura del SGSI?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Identificar los procesos de seguridad informática y de seguridad de la información actualmente implementados en la empresa para así auditarlos, hacer recomendaciones e implementar controles según el caso.

1.3.2 Objetivos específicos

Todos los objetivos específicos dependerán de las facilidades y el campo de acción que nos otorgue la empresa GNN7 TV.

- Identificar la razón por la que la gestión actual de la seguridad necesita estandarizar sus mecanismos de control.
- Determinar las causas por las que los mecanismos actuales de prevención y corrección están provocando fallos en el SGSI de la organización.
- Identificar las vulnerabilidades que provocan interrupciones y fallos en los servicios informáticos de la infraestructura del SGSI.

1.4 Justificación de la investigación

La seguridad informática actualmente se ha vuelto un punto crítico, por lo tanto la empresa requiere de un análisis acerca de su estado actual y lo recomendable es que sea efectuado por agentes externos. La oportunidad de realizar esta auditoría se da gracias a que la necesidad de la empresa se complementa con la nuestra, la empresa estaba en la búsqueda de un agente externo para realizar este proyecto y nosotros en la búsqueda de una empresa que nos permitiera hacer la investigación referente a seguridad informática y de la información.

1.5 Marco de referencia de la investigación

1.5.1 Marco teórico

A continuación haremos referencia a varios conceptos de vital importancia para el entendimiento y desarrollo de este estudio:

a) Auditoría informática

Es importante definir el término de auditoría, ya que el mismo se ha usado para referirse a una revisión cuyo único fin es detectar errores, fraudes, señalar fallas y como consecuencia recomendar mejoras, no obstante, la auditoría se puede definir como un proceso sistemático para evaluar y obtener de manera objetiva las evidencias relacionadas con informes sobre actividades o eventos a nivel informático. Pero, ¿Qué es la auditoría informática? Se podría definir como una serie de exámenes y revisiones

independientes, teóricas, periódicas o esporádicas de un sistema informático que abarca todo o algunas áreas de la organización cuya finalidad es analizar y evaluar la planificación, el control, la eficacia, la seguridad, la economía y la adecuación de la infraestructura informática de la empresa utilizando como herramientas de revisión los estándares y procedimientos en vigor, su idoneidad y el cumplimiento de éstos, de los objetivos fijados, los contratos y las normas legales aplicables, el grado de satisfacción de usuarios y directivos, los controles existentes y el análisis de riesgos.[4]

b) Información dentro de la organización

La información dentro de la organización es fundamental para el funcionamiento y quizá incluso sea un elemento decisivo para cualquier toma de decisión a nivel administrativo, técnico, financiero y general. El hecho de disponer de varios estándares para la revisión, control y auditoría de los procesos informáticos nos lleva a profundizar más sobre las distintas pautas existentes que podrían manejar las políticas para el funcionamiento óptimo del procesamiento de información.

c) Estándares y mejores prácticas

La importancia del uso de estándares y buenas prácticas cuando se trata de la seguridad de la información nos lleva a recalcar que los medios electrónicos informáticos como la Internet, redes de comunicaciones y computadoras es algo que se ha masificado tanto a nivel mundial como a nivel nacional en diferentes sectores como:

- Gobierno.
- Educación e investigación.
- Salud
- Comercio / Industria

[4] (Universidad Nacional Autónoma de México, 2010)

d) Motivos para el uso y prevención de ataques informáticos

Es importante la seguridad en cualquier sociedad, un pequeño porcentaje de la gente es maliciosa. Se dice que Internet tiene un crecimiento de usuarios en constante crecimiento y que sea cual sea el valor su porcentaje de usuarios maliciosos es menor al 1%[5]. Uno de los tantos motivos para la prevención y protección de ataques maliciosos consiste en asegurar lo siguiente:

- El derecho a la privacidad
- El derecho a estar informado
- Protección de los activos
- Proteger la información (Bases de datos, documentos digitales)
- Proteger los equipos (Sistemas de control, redes, etc.)
- Reforzar las leyes, políticas y procedimientos.

e) Diferentes organismos internacionales para la estandarización de la seguridad de la información e informática

- Organización Internacional para la Estandarización (ISO)
- Comisión Electrotécnica Internacional (IEC)
- Unión Internacional de Telecomunicaciones (ITU)
- Comité Consultivo Internacional Telegráfico y Telefónico (CCITT)
- Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)
- Instituto Nacional Estadounidense de Estándares (ANSI)
- Grupo de Trabajo de Ingeniería de Internet (IEFT)

[5] (Miniwatts Marketing Group, 2012)

f) Ventajas de los estándares de seguridad informática

- Homologación de aplicaciones
- Firmas digitales
- Posibilidad de interactuar con otros
- Existencia de un mejoramiento global

g) Estándar ISO/IEC 27001 – ISO/IEC 27002

Dentro de las certificaciones ISO para la seguridad de la información se encuentran 2 normas importantes para gestionar, controlar y preservar la buena práctica para la seguridad de la información, estas son la ISO/IEC 27001 y la ISO/IEC 27002

La norma ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información. La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales. Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.[6] La norma ISO/IEC 27002 es una guía de buenas prácticas de seguridad de la información que presenta una extensa serie de controles de seguridad. Es la única norma que no sólo cubre la problemática de la seguridad TI sino que hace una aproximación holística a la seguridad de la información corporativa, abarcando todas las funcionalidades de una organización en cuanto a su seguridad de la información. [7]

Tomando en cuenta que esta norma sólo hace recomendaciones mas no certifica y su detalle es en realidad sobre el uso de 133 controles de seguridad diferentes aplicados

[6] (Norma ISO 27001, 2005)
[7] (Norma ISO 27002, 2005)

en 11 áreas de control para la seguridad de la información. La ISO/IEC 27001 incorpora el típico "Plan – Do – Check – Act"[8] (PDCA) que significa "Planificar – Hacer – Controlar – Actuar" siendo este un enfoque de mejora continua:

- **Plan (planificar):** es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
- **Do (hacer):** es una fase que envuelve la implantación y operación de los controles.
- **Check (controlar):** es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
- **Act (actuar):** en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

h) Sistema de gestión de la seguridad de la información - SGSI

Es un conjunto de políticas claves de administración de la información dentro de una organización y es utilizado principalmente por la ISO/IEC 27001 para el planeamiento del diseño, implementación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad a la información, buscando asegurar la:

- Confidencialidad
- Integridad
- Disponibilidad

De los activos de información minimizando a la vez los riesgos de seguridad de la información. Como todo proceso de gestión, un SGSI debe seguir siendo eficiente

[8] (Norma ISO 27001, 2005)

durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno. La mejor definición de SGSI es descrito por la ISO/IEC 27001 y ISO/IEC 27002 y relaciona los estándares publicados por la ISO e IEC.

i) Ventajas de SGSI

El hecho de certificar un SGSI según la norma ISO/IEC 27001 puede aportar las siguientes ventajas a la organización:

- Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación.
- Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es de alta importancia.
- Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.
- El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.

Las organizaciones que simplemente cumplen la norma ISO/IEC 27001 o las recomendaciones de la norma del código profesional no logran estas ventajas, para eso existe el estándar ISO/IEC 27002.

j) Sistema informático

Un sistema informático, es el conjunto de partes interrelacionadas, hardware, software y de recurso humano que permite almacenar y procesar información. El hardware incluye computadoras o cualquier tipo de dispositivo electrónico inteligente, que consisten en procesadores, memoria, sistemas de almacenamiento externo, etc. El software incluye al sistema operativo, firmware y aplicaciones, siendo especialmente importante los sistemas de gestión de bases de datos. Por último el soporte humano incluye al personal técnico que crean y mantienen el sistema (analistas, programadores, operarios, etc.) y a los usuarios que lo utilizan.[9]

Un sistema informático seguro debe ser:

- Integro, con información modificable sólo por las personas autorizadas.
- Confidencial, los datos deben ser legibles solo para los usuarios autorizados.
- Irrefutable, el usuario no debe poder negar las acciones que realizó.
- Disponibilidad, debe ser estable y siempre accesible.

De todas formas, como en la mayoría de los ámbitos de la seguridad, lo primordial es la capacitación de los usuarios, una persona que conoce cómo protegerse de las amenazas sabrá utilizar sus recursos lo mejor posible para evitar ataques o accidentes.

k) Seguridad informática

La Seguridad Informática es la disciplina que se encarga de proteger la integridad y la privacidad total de la información almacenada en un sistema informático. Un sistema informático puede ser protegido desde un punto de vista lógico o físico. Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la

[9] (Definicion.de, 2012)

computadora del usuario (virus) o llegar por vía remota (hackers). Entre las herramientas más usuales de la seguridad informática, se encuentran los programas antivirus, los cortafuegos o firewalls, la encriptación de la información y el uso de contraseñas seguras.[10]

l) Firewall o cortafuegos

Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar el tráfico entre diferentes ámbitos sobre un conjunto de normas y criterios[11]. Los firewalls se caracterizan por lo siguiente:

- Pueden ser implementados como hardware, software o ambos.
- Se utilizan con frecuencia para evitar que usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets.
- Todos los mensajes que entren o salgan de la intranet pasan a través del firewall, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.
- Conectar al firewall a una tercera red, llamada zona desmilitarizada (DMZ), en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

m) Tipos de firewall

Nivel de aplicación de pasarela: Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores de transferencia de archivos (FTP). Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

[10] (Definicion.de, 2012)
[11] (Universidad de la República en Uruguay, 2013)

Circuito a nivel de pasarela: Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin ningún otro control. Permite el establecer una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.[12]

Firewall de capa de red o de filtrado de paquete: Funciona a nivel de red, capa 3 del modelo del sistema de interconexión abierto (OSI) y capa 2 del modelo TCP/IP, como filtro de paquetes del protocolo de internet (IP). A este nivel se realizan filtros según los campos con información de los paquetes IP: dirección origen y destino. A menudo en este firewall se permiten filtrados a nivel de transporte (capa 3 del modelo TCP/IP y capa 4 del modelo OSI), como el puerto de origen y destino, o a nivel de enlace de datos (no existe en el modelo TCP/IP y capa 2 del modelo OSI).[13]

Firewall de capa de aplicación: Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de esta manera los filtrados se pueden adaptar a las características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico web, se pueden realizar filtrados según la dirección localizadora uniforme (URL) a la que se está intentando acceder. Un firewall a nivel 7 de tráfico suele denominarse proxy, este permite que los computadores que son parte de la infraestructura de red accedan a Internet de forma controlada y segura. Un proxy oculta las direcciones IP reales de la red.[14]

Firewall personal: Es un caso particular de firewall que se instala como un programa normal en un computador, se pueden filtrar las comunicaciones entre dicho computador y el resto de los equipos de la red. Se usa por tanto, a nivel personal. Un firewall personal correctamente configurado permite un nivel de protección necesario en la red, pero que en ningún caso debe considerarse como único mecanismo de protección.[15]

[12] (Universidad de la República en Uruguay, 2013)
[13] (Universidad de la República en Uruguay, 2013)
[14] (Universidad de la República en Uruguay, 2013)
[15] (Universidad de la República en Uruguay, 2013)

n) Protección de datos y registro de su propagación a través de cualquier medio.

Las soluciones de prevención de pérdida de datos (DLP), ayudan a reducir el riesgo de pérdida o de robo de información sensible. Los sistemas de DLP administran a los clientes de la red, incluyendo ordenadores portátiles, estaciones de trabajo y dispositivos periféricos, y controlan las operaciones que estos efectúan, con datos almacenados localmente y en la red. Estos sistemas pueden igualmente validar el acceso a datos, mediante medios extraíbles, como memorias flash, y definir lo que cada usuario está autorizado a realizar. [16]

El cifrado del escritorio protege los datos sensibles estáticos y en tránsito, de tal manera que puedan acceder a los mismos únicamente el (los) usuario(s) predeterminados, que presenten las credenciales requeridas. Éste puede aplicarse a múltiples capas de almacenamiento de datos, dependiendo de las necesidades de seguridad de la organización. Algunas de las aplicaciones de cifrado de escritorio más utilizadas cifran archivos, discos completos y correo electrónico. Puede igualmente cifrarse los ordenadores portátiles y dispositivos portables, para prevenir la pérdida de datos.

o) Alojamiento web

Es la manera de poder almacenar información, imágenes, o cualquier contenido en Internet, con el fin de respaldar o tener disponible la información y permitir un trabajo dinámico en las labores del departamento de TI. Es el servicio que se provee a empresas o usuarios comunes para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía web. Es una analogía de hospedaje o alojamiento en hoteles o habitaciones donde uno ocupa un lugar específico, en este caso la analogía alojamiento web se refiere al lugar que ocupa una página web, sistema, correo electrónico o archivos, en un servidor que por lo general hospeda varias aplicaciones o páginas web. Las compañías que proporcionan espacio de un servidor a sus clientes se suelen denominar con el término en inglés web host. [17]

[16] (Gemalto, 2010)
[17] (Super Hosting, 2011)

El hospedaje web aunque no es necesariamente un servicio, se ha convertido en un negocio lucrativo para las compañías de Internet alrededor del mundo. Se puede definir como "un lugar para tu página web o correos electrónicos", aunque esta definición simplifica de manera conceptual el hecho de que el alojamiento web es en realidad espacio en Internet para prácticamente cualquier tipo de información, sea archivos, sistemas, correos electrónicos, videos etc.

p) Protección anti-malware

Malware, también llamado código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos. El software se considera malware en función de los efectos que provoque en un computador. El término malware incluye virus, gusanos, troyanos, la mayor parte de los rootkits, spyware, adware intrusivo, crimeware y otros software maliciosos e indeseables; malware no es lo mismo que software defectuoso, este último contiene bugs peligrosos, pero no de forma intencionada.[18]

q) Virtualización

La virtualización es la creación a través de software de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red. Dicho de otra manera, se refiere a la abstracción de los recursos de una computadora, creando una capa de abstracción entre el hardware de la máquina física y el sistema operativo de la máquina virtual, dividiéndose el recurso en uno o más entornos de ejecución. Esta capa de software maneja, gestiona y arbitra los cuatro recursos principales de una computadora (CPU, memoria, disco y conexiones de red) y así podrá repartir

[18] (Universidad Nacional Autónoma de México, 2013)

dinámicamente dichos recursos entre todas las máquinas virtuales definidas en el computador central. Esto hace que se puedan tener varios ordenadores virtuales ejecutándose en el mismo ordenador físico.[19]

La virtualización se encarga de crear una interfaz externa que encapsula una implementación subyacente mediante la combinación de recursos en localizaciones físicas diferentes, o por medio de la simplificación del sistema de control. Un avanzado desarrollo de nuevas plataformas y tecnologías de virtualización ha hecho que en los últimos años se haya vuelto a prestar atención a este concepto. La máquina virtual en general simula una plataforma de hardware autónoma incluyendo un sistema operativo completo que se ejecuta como si estuviera instalado. Típicamente varias máquinas virtuales operan en un computador central. Existen diferentes formas de virtualización, es posible virtualizar el hardware de servidor, el software de servidor, virtualizar sesiones de usuario, virtualizar aplicaciones y también se pueden crear máquinas virtuales en una computadora de escritorio. Con la consolidación del modelo de la informática en la nube, la virtualización ha pasado a ser un componente fundamental, especialmente en lo que se denomina infraestructura de nube privada.[20]

r) Monitoreo de red

El término monitoreo de red describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico u otras alarmas. Es un subconjunto de funciones de la administración de redes. Mientras que un sistema de detección de intrusos monitorea una red por amenazas del exterior (externas a la red), un sistema de monitoreo de red busca problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red (u otros dispositivos). Por ejemplo, para determinar el estatus de un servidor web, software de monitoreo puede enviar, periódicamente, peticiones HTTP (Protocolo de Transferencia de Hipertexto) para obtener páginas; para un servidor de

[19] (Capacity Information Technology Academy, 2012)
[20] (Capacity Information Technology Academy, 2012)

correo electrónico, enviar mensajes mediante SMTP (Protocolo de Transferencia de Correo Simple), para luego ser retirados mediante IMAP (Protocolo de Acceso a Mensajes de Internet) o POP3 (Protocolo Post Office).[21]

Comúnmente, los datos evaluados son tiempo de respuesta y disponibilidad, aunque estadísticas tales como consistencia y fiabilidad han ganado popularidad. La generalizada instalación de dispositivos de optimización para redes de área extensa tiene un efecto adverso en la mayoría del software de monitoreo, especialmente al intentar medir el tiempo de respuesta de punto a punto de manera precisa, dado el límite visibilidad de ida y vuelta. Todos los eventos en la red pueden variar, se puede plantear un sistema de alarmas que se envíen al administrador o la ejecución automática de mecanismos de controles de fallas, etcétera.

s) Administrador de red

Los administradores de red mantienen el hardware y software de la red, esto incluye el despliegue, mantenimiento y monitoreo de la red: switch, router, firewall, etc. Las actividades de administración de una red por lo general incluyen la asignación de direcciones, asignación de protocolos de ruteo y configuración de tablas de ruteo así como, configuración de autenticación y autorización de los servicios.

Frecuentemente se incluyen algunas otras actividades como el mantenimiento de las instalaciones de red tales como los controladores y ajustes de las computadoras e impresoras. A veces también se incluye el mantenimiento de algunos tipos de servidores como VPN, sistemas detectores de intrusos, etc. Los analistas y especialistas de red se concentran en el diseño y seguridad de la red, particularmente en la resolución de problemas o depuración de problemas relacionados con la red. Su trabajo también incluye el mantenimiento de la infraestructura de autorización a la red.[22]

[21] (Universidad Nacional Autónoma de México, 2005)
[22] (Microsoft, 2013)

Algunas funciones de administración de red incluyen:

- Proporcionar servicios de soporte
- Asegurarse de que la red sea utilizada eficientemente
- Asegurarse que los objetivos de calidad de servicio se alcancen.

1.5.2 Marco conceptual

Inventario de recursos informáticos: El inventario de recursos informáticos es el proceso de recopilar información de las características de los equipos y aplicativos informáticos. Esto permite evaluar el impacto de los recursos informáticos en los procesos críticos de la empresa, los recursos disponibles, la posibilidad de implementar soluciones, tomar acciones correctivas y desarrollar planes de contingencias.[23]

Seguridad informática: Es el conjunto de procedimientos, estrategias y herramientas que permiten garantizar la integridad, disponibilidad y confidencialidad de la información de una organización.[24]

Seguridad de la información: Son todas las medidas preventivas y reactivas del hombre, de una organización y de sistemas tecnológicos que permiten proteger la información garantizando confidencialidad, disponibilidad e integridad de la misma.[25]

Red de comunicación: Es un conjunto de dispositivos físicos y programas mediante los cuales diferentes computadoras pueden comunicarse con sus recursos.[26]

[23] (Eprints, 2003)
[24] (Julio Rios, 2003)
[25] (Asociación Española para la Calidad, 2013)
[26] (AngelFire, 2003)

Vulnerabilidad informática: Debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencias del sistema o de sus datos y aplicaciones. [27]

Antivirus: Son programas cuyo objetivo es detectar y/o eliminar virus informáticos. Nacieron durante la década de 1980. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de malware, como spyware, rootkit, etc.[28]

Firewall: Parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas puede a la vez ser también un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.[29]

Prevención de pérdida/fuga de información: Termino que se emplea para la corrección de vulnerabilidades en cuanto a la fuga de información, el cual utiliza un amplio conjunto de productos innovadores centrados en la integración y capacidad de gestión de la próxima generación de tecnologías de prevención de pérdida de datos (DLP, Data Loss Prevention); se han diseñado específicamente para evitar este tipo de desastres[30]. Independientemente de donde estén almacenados los datos, una iniciativa para DLP puede reducir el riesgo de la pérdida de información, además de servir de ayuda para identificar riesgos, establecer políticas y procesos, educar a los usuarios e integrar tecnologías y controles para potenciar la seguridad.

[27] (WebQuest, 2010)
[28] (Microsoft, 2013)
[29] (Universidad de la República en Uruguay, 2013)
[30] (Gemalto, 2010)

1.6 Formulación de la hipótesis y variables

1.6.1 Hipótesis general

La mala gestión de los mecanismos actualmente implementados en el SGSI de la empresa no permite cubrir las necesidades de protección contra amenazas internas y externas de seguridad.

1.6.2 Hipótesis particulares

- El esquema del SGSI actual no se rige bajo ningún estándar internacional, lo cual produce impactos negativos de seguridad.
- Al no estar estandarizado el SGSI los mecanismos de control preventivos y correctivos no brindan las garantías necesarias, por lo que se generan fallos, interrupciones y fuga de información.
- Los fallos en la red, gestión de procesos mal implementados y la falta de monitoreo de eventos externos generan interrupciones en los servicios informáticos de la infraestructura del SGSI los cuales se vuelven deficientes.

1.6.3 Matriz causa y efecto

Formulación del Problema	Objetivo general	Hipótesis general
¿Cuál es la razón para determinar que los procesos actuales de seguridad informática y de la información no son los adecuados para la organización?	Identificar los procesos de seguridad informática ya implementados que no están cubriendo las necesidades de protección de información de la empresa.	La mala gestión de los mecanismos actualmente implementados en el SGSI de la empresa no permite cubrir las necesidades de protección contra amenazas internas y externas de seguridad.

Sistematización del problema	Objetivos específicos	Hipótesis específicas
¿Por qué la gestión actual de la seguridad de la información que lleva acabo la empresa no es eficiente?	Identificar la razón por la que la gestión actual de la seguridad necesita estandarizar sus mecanismos de control.	El esquema del SGSI actual no se rige bajo ningún estándar internacional, lo cual produce impactos negativos de seguridad.
¿Por qué la no estandarización del SGSI causa problemas de seguridad en la empresa?	Determinar las causas por las que los mecanismos actuales de prevención y corrección están provocando fallos en el SGSI de la organización.	Al no estar estandarizado el SGSI los mecanismos de control preventivos y correctivos no brindan las garantías necesarias, por lo que se generan fallos, interrupciones y fuga de información.
¿Cuáles son los factores que inciden para que se presenten interrupciones y fallos en la infraestructura del SGSI?	Identificar las vulnerabilidades que provocan interrupciones y fallos en los servicios informáticos de la infraestructura del SGSI	Los fallos en la red, gestión de procesos mal implementados y la falta de monitoreo de eventos externos generan interrupciones en los servicios informáticos de la infraestructura del SGSI los cuales se vuelven deficientes.

Tabla #1: Matriz causa y efecto

Elaborado por: Autores

1.6.4 Variables

1.6.4.1 Variables independientes

Mecanismos empleados para brindar seguridad a la información.

1.6.4.2 Variables dependientes

Pérdida monetaria y de tiempo debido a interrupciones de red y vulnerabilidades de la seguridad informática y de la información.

1.7 Aspectos metodológicos de la investigación

1.7.1 Tipo de estudio

El plan de mejoras para planificar, solucionar y controlar la seguridad informática y de la información dentro de la empresa está basado en los siguientes tipos de estudio:

Investigación exploratoria: La finalidad de realizar esta investigación será analizar los problemas de seguridad informática y de la información dentro de la organización, previo a la investigación los antecedentes o datos similares eran escasos y por ende se tuvo que explorar todos los temas referentes al desarrollo y gestión de la seguridad.

Investigación no experimental: Los sujetos de estudio que en este caso son el personal de la organización, fueron observados en su contexto natural y en su realidad cotidiana. No se los sometió a un experimento en particular sobre la falta de procedimientos para resolver casos de seguridad informática y de la información.

Investigación de campo: El estudio se realizó en el ambiente natural en el cual se desenvuelven los encargados del SGSI, mediante entrevistas se pudo obtener datos relevantes de la situación actual de la seguridad informática y de la información.

1.7.2 Método de investigación

De acuerdo al análisis de la investigación y acciones correctivas que van a ser presentadas para la evaluación y mejor toma de decisión en el ámbito de la seguridad informática, hemos encontrado que lo realizaremos basándonos en los siguientes métodos de investigación:

Método inductivo - deductivo: De nuestras hipótesis e ideas debemos llegar a una conclusión, para que así tanto nosotros como la empresa podamos tomar las acciones correctivas a seguir para asegurar el cumplimiento de lo propuesto.

Método analítico - sintético: Tomaremos como guía otras investigaciones y la utilización de estándares para con ello determinar en base a análisis previos el cumplimiento de las recomendaciones de los controles y arreglos para la seguridad de la información.

Método observativo: Este método es empleado para la detección visual de falencias de seguridad física y mala gestión de procesos como: toma de inventario, reparación de activos y demás, que pudieron ser catalogadas como riesgos de la seguridad de información.

1.7.3 Fuentes y técnicas para la recolección de información

Entrevista al Jefe del departamento de TI

Se realizó una única entrevista al jefe del departamento de TI, con los demás miembros del departamento se mantuvieron conversaciones durante el desarrollo de la auditoría, todo fue relacionado al desempeño actual del sistema de seguridad informática y de la información. Para efectos de este trabajo el personal que participó fue todo el personal del departamento de TI de la empresa, puesto que conocen con gran detalle el estado actual de la gestión de la seguridad de la información de la organización.

Observación - Análisis del SGSI

El proceso de recopilación de información es la parte más extensa del proceso de investigación ya que mediante varios sistemas pudimos obtener el estado actual de la organización; se revisó el software y documentación que tiene el departamento de TI.

1.7.4 Población y muestra

- **Población**

  Personal del departamento de TI, los cuales conocen al detalle la situación actual del SGSI de la empresa.

- **Muestra**

  La totalidad del personal de TI, el departamento cuenta con 6 personas donde cada uno cumple con funciones específicas en la administración del SGSI.

CAPÍTULO 2

2. ANÁLISIS, PRESENTACIÓN DE RESULTADOS Y DIAGNÓSTICO

2.1 Análisis de la situación actual

La gran mayoría de las vulnerabilidades que se presentan en la empresa se debe al poco conocimiento e importancia que representa la seguridad de la información para los gerentes, los cuales son los responsables directos del estancamiento tecnológico que puede sufrir una organización, es difícil lograr que entiendan que la prioridad del negocio no es solo el ingreso económico sino también los procesos intermedios.

A este nivel, resulta imprescindible conocer la problemática, lo que determina la necesidad de efectuar un estudio de seguridad o, al menos, una auditoría competente, el resultado de llevar acabo la ejecución de procesos de auditoría informática, dará

como resultado conocer con exactitud los diversos riesgos y las diferentes soluciones posibles ante alguna vulnerabilidad o amenaza, así como del coste de cada una. Sobre la base de estos elementos, la dirección del organismo puede ya plantear los objetivos que resuelvan, en el espacio y en el tiempo, la problemática de seguridad existente, lo que se traducirá en el establecimiento de prioridades y plazos para su remediación.

Las empresas que no cuentan con el conocimiento acerca de sus vulnerabilidades y puntos débiles que pueden presentar pérdida de información, ya sea por un evento natural, por el ataque de hackers, trabajadores que se van de la firma o personas que se lucran con la información, debido a la mala implementación de políticas y normas de seguridad de la información; por lo tanto se le debe dar mucha importancia a la inversión de recursos sistemas informáticos y a su vez contar con el personal certificado en prácticas de seguridad informática y resguardo de información.

2.2 Auditoría en base a controles de la Norma ISO 27002

Según el requerimiento del jefe del área de tecnologías de la información de la empresa, se acordó realizar una auditoría en base a cuatro dominios de la norma ISO 27002, enfocándose a objetivos de control puntuales que están dentro de la prioridad del SGSI y que están dentro del campo de acción del departamento de TI:

- Responsabilidad sobre los activos
- Seguridad de los equipos
- Responsabilidad y procedimientos de operación
- Protección contra el código malicioso
- Copias de seguridad
- Gestión de la seguridad de la red
- Supervisión del SGSI

- Controles de acceso
- Gestión de acceso de los usuarios
- Control de acceso a los sistemas operativos
- Control de acceso a las aplicaciones

2.3 Objetivo de la auditoria

Realizar una auditoría/consultoría al SGSI de la empresa en base a los objetivos de control de la norma ISO 27002 definidos previamente.

- Conseguir y mantener la protección apropiada de los activos organizacionales; todos los activos deben estar inventariados, codificados y tener un propietario designado.
- Evitar la pérdida, daño, robo o exposición de los activos y la interrupción de las actividades de la organización.
- Asegurar lo operación correcta y segura de los medios de procesamiento de la información.
- Proteger la integridad del software y la información. Se requiere mecanismos para prevenir y detectar la introducción de código malicioso y programas no autorizados.
- Mantener la integridad y disponibilidad de los sistemas de información y servicios de comunicación.
- Proteger la información en las redes y la infraestructura de soporte.
- Prevenir la divulgación no autorizada, modificación, eliminación o destrucción no autorizada de recursos, y las interrupciones de las actividades del negocio. La medida debería ser controlada y físicamente protegida.

- Detectar las actividades de procesamiento de la información no autorizadas. Los sistemas deben ser monitoreados y los eventos de la seguridad de la información deben ser registrados.

- Controlar el acceso a la información y los procesos del negocio deben ser controladas sobre la base de los requerimientos de seguridad y del negocio.

- Evitar el acceso no autorizado a los sistemas de información. Deben establecerse procedimientos formales para controlar la distribución de los derechos de acceso a los servicios de sistemas de información.

- Evitar el acceso no autorizado de los usuarios y la exposición o el robo de la información de los sistemas de información. La cooperación de los usuarios autorizados es esencial para la seguridad efectiva.

- Prevenir accesos no autorizados a los servicios de la red. Debe controlarse el acceso a los servicios de la red internos y externos.

- Evitar los accesos no autorizados a los sistemas operativos.

- Evitar el acceso no autorizado y restringir el acceso a los sistemas de información.

2.4 Estructura del área de TI de la empresa

2.4.1 Personal de TI y sus funciones

El departamento de TI cuenta con 6 miembros y estos son sus cargos:

- Jefe de tecnologías de la información

- Coordinador de infraestructura y redes

- Coordinador de sistemas multimedia

- Coordinador de seguridad informática y helpdesk.

- Asistente de sistemas
- Asistente de sistemas

2.4.2 Organigrama TI de la empresa

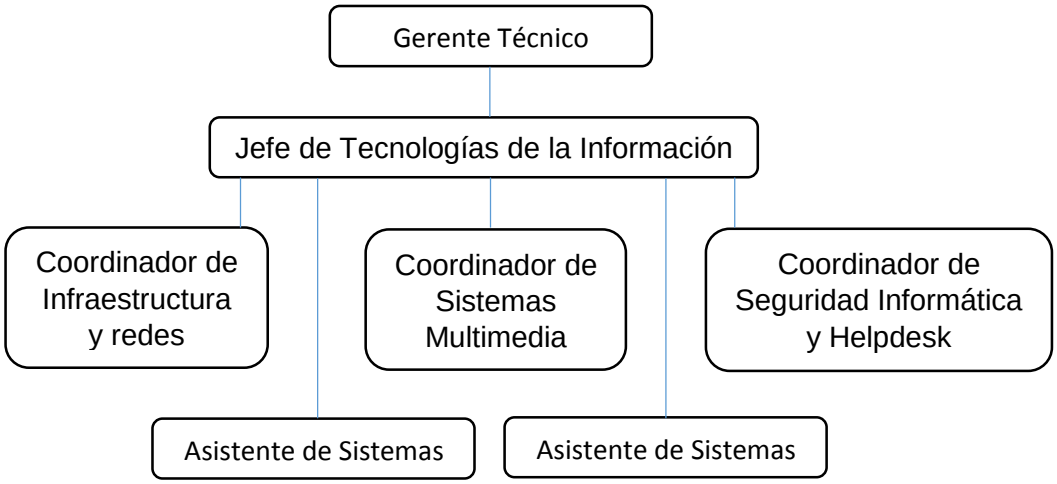


Figura #2.1: Organigrama TI de la empresa

Nota: Información obtenida del Jefe del departamento de TI de GNN7 TV, elaborado por: Autores

2.5 Diagnóstico

2.5.1 Información recopilada

Para el desarrollo de esta auditoría y poder dar un diagnóstico se conversó con el responsable del departamento de TI y cada uno de sus miembros, se pudo comprobar que no se mantienen normas de seguridad de la información en la empresa, tomando como referencia los objetivos de control de la norma ISO 27002 que se especificaron en el punto 2.2. El estado de GNN7 TV se resume en la entrevista presentada a continuación, esta fue realizada al responsable del departamento de TI previa al desarrollo de esta auditoría y por medio de la información adquirida se pudo realizar un diagnóstico que permitió que este proyecto de tesis sea viable.

Entrevista realizada al responsable del departamento de TI de GNN7 TV

a) Sobre políticas de seguridad de la información

¿Cuentan GNN7 TV con políticas de seguridad de la información?

Si, existen políticas de seguridad informática y de la información definidas a manera general en las cuales existen prohibiciones y sanciones si no son acatadas por el personal de GNN7 TV en general.

¿Existen controles para comprobar el cumplimiento de sus políticas?

Si, existen controles definidos pero no implementados en su totalidad. Muchas de las políticas expuestas y aprobadas por Gerencia general son cumplidas pero no comprobadas al no existir un seguimiento de las mimas.

¿Todo el personal de GNN7 TV tiene conocimiento de las políticas de seguridad de la información?

El personal nuevo que ingresa a GNN7 recibe charlas de inducción para conocer las políticas de seguridad informática y de la información, pero el personal que ha estado laborando algunos años en la empresa no conoce en su totalidad las políticas de seguridad informática.

b) Sobre la gestión de activos

¿Los activos informáticos están debidamente registrados por el departamento de TI en un inventario?

Si, existe un control de ingreso de información de los activos de información por parte del área de administración de activos fijos de GNN7 TV, pero como departamento de TI llevamos un control eventual, básico y no gestionado ni controlado del registro de activos de computación.

¿Este inventario está automatizado?

El inventario no está automatizado debido a que no contamos con un software que pueda facilitarnos la tarea de administración y control de los activos de computación.

¿El inventario de activos informáticos se actualiza periódicamente?

No necesariamente, la tarea de actualización se realiza cada año o pasando 2 dependiendo de la necesidad de algún requerimiento especifico de dicha información debido a que en varias ocasiones por tema de control de compras se requiere conocer si los activos se encuentran en buen estado, quienes son los custodios de los mismos, cambios de equipos por garantías y equipos que se dan de baja por el tiempo de uso.

c) Sobre el personal de GNN7 TV

¿Los incidentes en los activos informáticos son reportados rápidamente por los usuarios?

Si, los usuarios en general reportan todos los incidentes relacionados con los activos.

¿El departamento de TI cuenta con actas de responsabilidad sobre los activos firmadas por cada usuario de GNN7 TV?

No, el procedimiento de asignación de activos de computación no se encuentra definido por procesos de entrega con actas de responsabilidad sobre su uso.

d) Sobre la seguridad física y del entorno

¿GNN7 TV cuenta con mecanismos de respaldo del servicio eléctrico para garantizar la continuidad de las operaciones?

Si, existen mecanismos de respaldo del servicio eléctrico que funciona correctamente cada vez que exista alguna interrupción con la energía eléctrica.

¿Se realiza mantenimiento periódico al hardware y software de GNN7 TV?

No, el mantenimiento de los equipos se realiza solo si por sus condiciones de mal funcionamiento lo amerita; esto quiere decir que no son periódicas y tampoco hay algún tipo tarea o gestión creada para que este proceso sea preventivo.

¿Existen controles para los activos informáticos al estar fuera de GNN7 TV?

No, no existen controles o normas definidas para equipos o activos de computación de propiedad de la empresa cuando están fuera de las instalaciones de la empresa.

¿Hay procedimientos para la reutilización de activos informáticos y para cuando estos son dados de baja?

Si, la mayoría de los equipos dependiendo de sus características pueden ser reutilizados o dados de baja; tal proceso se realiza en conjunto con el área de activos fijos para los registros de auditoría general.

e) Sobre la gestión de comunicaciones y operaciones

¿Tienen manuales de operación para cada uno de los sistemas informáticos?

No, contamos con pocos manuales de operación de los sistemas informáticos.

¿El personal de TI registra los cambios hechos en los sistemas informáticos (aplicaciones, software y sistema operativo)?

No, el departamento no tiene registros de incidentes sobre los sistemas informáticos.

¿Están debidamente segregadas las tareas del personal TI?

Si, cada uno sabe sus funciones y tareas a cumplir como parte de su trabajo.

¿GNN7 TV cuenta con controles contra software malicioso (Firewall, parches del SO, antivirus, antispyware, etc.)?

Si, contamos con herramientas de monitoreo y otras instaladas en las estaciones de trabajo (Anti-virus) para la detección de código malicioso y virus.

¿Cuentan con mecanismos de respaldo para los medios de almacenamiento?

Si, existen mecanismos generales definidos para el respaldo de información tanto de estaciones de trabajo como de servidores.

¿Existen controles para la buena administración de los recursos de red (ancho de banda, direccionamiento IP, etc.)?

Si, GNN7 TV cuenta con herramientas de control y monitoreo del uso general del ancho de banda; obteniendo con esto índices de consumo de Internet por usuarios así como también controles de direccionamiento IP asignados a los mismos.

¿El área de TI ha implementado controles de monitoreo de actividades de red?

Si, el departamento cuenta con controles de monitoreo de sucesos en la red.

¿Registran actividades y eventos de seguridad en los sistemas de información?

Si, en la mayoría de los casos las actividades de seguridad informática relacionadas a los sistemas de información son registradas por el personal responsable del área de TI.

¿Se registra la actividad de los usuarios y administradores en los sistemas de información de GNN7 TV?

Si, se lleva a cabo registros de actividades de los usuarios sobre los recursos informáticos a los que puedan acceder.

f) Sobre los controles de acceso

¿Para los sistemas de información existen políticas de control de acceso?

Si, la mayoría de los sistemas de información tienen políticas de control de acceso.

¿Las políticas de control de acceso son aplicadas?

Si, las políticas son aplicadas en su totalidad por todos los miembros de GNN7 TV.

¿Hay un registro de los accesos otorgados a los sistemas informáticos?

Si, aunque este registro de accesos es actualizado esporádicamente.

¿Se aplican controles para el registro de nuevos usuarios?

Si, los controles para el registro de usuarios se aplican cada vez exista algún incidente con los mismos ya sea creación, eliminación o modificación de algún usuario.

¿Cuentan con procedimientos para agregar o quitar accesos a los usuarios a los sistemas de información?

Si, el agregar o quitar accesos a los usuarios a los sistemas de información es gestionado y revisado por el personal del área de TI.

¿Todas las aplicaciones tienen ID y contraseña para dar acceso a los usuarios?

Si, el uso de usuarios y contraseñas es único para todo el personal de GNN7 TV.

¿Hay políticas para la creación de contraseñas?

Si, existen lineamientos a cumplir para la creación de contraseñas.

¿El departamento de TI restringe y controla las aplicaciones autorizadas?

Si, existen aplicaciones permitidas dependiendo del perfil del usuario así como también accesos a sistemas de información o utilización de algún recurso.

¿Hay controles para las sesiones inactivas de los usuarios?

Si, existen mecanismos definidos para gestionar sesiones activas por usuarios.

g) Sobre el reporte de incidentes

¿GNN7 TV cuenta con un procedimiento formal para reportes de incidentes?

Si, contamos con un procedimiento general pero no formal de reportes de incidentes.

¿El departamento de TI tiene una herramienta de gestión de incidentes?

No, no contamos con herramientas de registro de incidentes.

¿Al reporta un incidente de seguridad se cuenta con un plan de respuesta?

Si, existen planes de respuesta de seguridad establecidos para gestionar cualquier incidente ocurrido con los sistemas de información.

h) Sobre los planes de continuidad

¿Se realizan pruebas, mantenimiento y evaluación constante de los planes de continuidad de las operaciones?

No, no existen planes de continuidad definidos y por ende no se realizan ni simulacros o pruebas de dichos planes.

2.5.2 Diagnóstico previo

Luego de mantener conversaciones con cada uno de los miembros del departamento de TI y sobre todo en base a la entrevista hecha al responsable del departamento se concluyó que sus procedimientos actuales carecen en su mayoría de controles que hagan viable una buena gestión de los mismos, además es vulnerable a sufrir pérdida o robo de información ya que los controles actualmente implementados no son del todo eficientes, es por esto que se llegó a la conclusión de que es necesaria una auditoría y posterior corrección de las falencias de su SGSI, como antes se mencionó la base de este proyecto serán varios controles de la norma ISO 27002, el objetivo es estandarizar los procesos de GNN7 TV para en el futuro poder obtener la certificación en la misma.

CAPÍTULO 3

3. IMPLEMENTACIÓN DE LA AUDITORIA/CONSULTORÍA

3.1 Desarrollo de la auditoria

La auditoría será desarrollada en las instalaciones de GNN7 TV, todas las políticas propuestas se basarán en los objetivos previamente definidos y se ajustarán a las necesidades de GNN7 TV. Los dominios de la norma que serán base de este proyecto:

- Gestión de activos.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de acceso.

El resultado de esta auditoría y las soluciones propuestas o implementadas serán expuestos en este documento, pero las políticas entregadas al departamento de TI como parte de dicha solución serán modificadas para poder ser incluidas en este documento debido a la confidencialidad acordada.

3.2 Dominio - Gestión de activos

El objetivo de este dominio de control es regularizar la gestión de activos informáticos en GNN7 TV aplicando los controles de la Norma ISO 27002, esto contempla los siguientes puntos:

- Identificación e inventariado de los activos de computación de la organización.
- Documentar el uso aceptable de los activos de computación de la organización.
- La identificación de un custodio.

3.2.1 Objetivo de Control - Responsabilidad de los activos

Objetivo: Lograr y mantener una apropiada protección de los activos organizacionales. Todos los activos debieran ser inventariados y contar con un propietario nombrado, los propietarios debieran identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados.

3.2.1.1 Auditoria - Inventario de activos

Objetivo

El objetivo de este control es proporcionar al departamento de TI una guía metodológica que permita y facilite realizar la toma del inventario de todos los activos informáticos (hardware y software), con el fin de gestionar y optimizar los recursos tecnológicos de GNN7 TV.

Alcance

El alcance de este control es recopilar información necesaria sobre los recursos computacionales de GNN7 TV y así poder obtener reportes sobre el estado actual de los mismos. Con tal propósito se deben realizar los siguientes inventarios:

- Computadoras y software instalado, que permitirá identificar y registrar las características técnicas y administrativas del hardware y software de cada computadora.
- Equipos de red, que permitirá identificar y registrar todos los dispositivos que operan en la red empresarial.
- Aplicaciones, que permitirá identificar y registrar cada aplicación detallando sus funciones, características técnicas y administrativas.

Auditoría

El área de TI actualmente no ejecuta un adecuado proceso para la toma de inventario de equipos y accesorios de computación adquiridos, arrendados, donados, recibidos y/o dados de baja, lo cual impide controlar y gestionar los recursos informáticos de GNN7 TV de forma correcta, lo que conlleva a no obtener un registro de la cantidad, ni las características de los equipos informáticos de la institución.

Estas son las falencias detectadas en el actual proceso de toma de inventario:

- El inventario de equipos de computación se lleva a cabo en un periodo de tiempo excesivamente largos (una vez al año).
- No cuentan con reportes actualizados de toda la información relacionada a la gestión de activos.
- El departamento de TI no cuenta con una herramienta que faciliten o automatice la ejecución del inventario.
- No se encuentran establecidos mecanismos para dar de baja a los dispositivos de computación.

Diagrama de proceso de inventario de activos (actual)

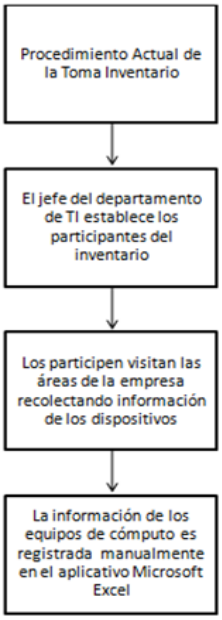


Figura #3.1: Diagrama de proceso de inventario de activos (actual)

Nota: Información obtenida del Jefe del departamento de TI de GNN7 TV, elaborado por: Autores

Recomendaciones

Procedimientos previos al inventario

- Elaboración de un plan de trabajo para la toma de activos de computación.
- Efectuar un cronograma de actividades de registro de activos de computación.
- Diseño de estrategias para la ejecución del inventario general de activos de computación.
- Designación del responsable de la ejecución del proceso de toma de inventario de activos de computación.
- El personal designado deberá ser instruido en el llenado de los formatos de la toma de activos de computación.
- Establecer un listado de los equipos y accesorios de computación.

- Revisión del “Manual de procedimiento para el levantamiento de inventario de activos informáticos” (Ver 3.2.1.2), para determinar si las instrucciones son adecuadas y claras. Es recomendable solicitar y revisar el documento días anteriores al inventario.

- Verificar que el departamento de TI comunicó con anterioridad a los participantes la documentación para la toma de inventario.

- Comprobar si GNN7 TV tiene bajo custodia inventario de terceros. De ser así, asegurarse que este inventario no pueda ser incluido para cubrir posibles faltantes.

- Confirmar que los equipos de computación en estado obsoleto, dañado, discontinuado o de lenta rotación, se encuentran debidamente identificados y separados.

- Realizar recorridos por las instalaciones de GNN7 TV para determinar las áreas en donde se encuentran ubicados los equipos de computación.

- Observar la correcta estructuración de los grupos de levantamiento de inventario; es recomendable que cada grupo incluya una persona familiarizada con los equipos de computación. Ej.: personal del departamento de TI.

- Corroborar si existe una adecuada segregación de tareas entre las personas responsables del inventario y los encargados de ingresar los registros.

Procedimiento Durante la Ejecución del Inventario

- Verificar que la toma del inventario se ejecuta de acuerdo al “Manual de procedimiento para el levantamiento de inventario de activos informáticos” (Ver 3.2.1.2).

- Supervisar el levantamiento de información de los dispositivos de computación.

- Ingreso de datos a cargo del responsable del área de TI de la toma de activos de computación.

- Durante la ejecución del proceso de inventario, el jefe del departamento de TI solicitará informes para validar la información recopilada hasta el momento.
- Examinar las medidas de seguridad para el acceso a las distintas áreas dentro de GNN7 TV para realizar la toma del inventario de activos de computación.
- Identificar y cuantificar los equipos de computación obsoletos, dañados, descontinuados o de lenta rotación.

Procedimientos finales del inventario

- Registrar los datos obtenidos del inventario de activos de computación en un sistema de información que facilite la emisión de resultados.
- La verificación de los datos ingresados debe estar acorde al listado de los recursos previamente obtenidos, para evitar omisiones y errores. El personal encargado es el responsable de la verificación de la información obtenida.
- Garantizar la calidad de los datos recolectados en el inventario de activos de computación, durante todas las etapas del procesamiento.
- Cumplir con los tiempos establecidos para obtención de resultados de la toma de activos de computación.
- Establecer los métodos y procedimientos en el tratamiento de la información recolectada en el inventario de activos de computación.
- Realizar la evaluación de la información obtenida de la toma del inventario de activos de computación.
- Elaborar los resultados del inventario para la evaluación del impacto y priorización de proyectos.
- Plantear alternativas de solución a los resultados obtenidos de la evaluación del Inventario de activos de computación.
- Informar permanentemente al jefe del área de TI de las actividades, avances y problemas que deriven de la realización del inventario.

Automatización del inventario

Luego de analizar las necesidades y falencias en la toma de inventario de activos de computación del departamento de TI se concluyó que la herramienta adecuada para el proceso de automatización del inventario de activos es el programa "Spiceworks", dicha aplicativo es capaz de inventariar, controlar, gestionar e informar sobre los activos de software y hardware de GNN7 TV, recopilando información, haciendo diagnósticos y generando reportes referidos a la cantidad de equipos, dispositivos conectados, servidores y otros elementos. Otra herramienta útil de este programa es su sistema de alertas, sirve notificar sobre aspectos relevantes como la falta de antivirus, el poco espacio en disco o la indisponibilidad de algún servicio. Para la implementación y buen uso de esta herramienta revisar el "Manual de usuario - Spiceworks" (Ver 3.2.1.3). Spiceworks cuenta con las siguientes opciones para la toma de inventario de activos de computación:

- Escaneo de los dispositivos de la red corporativa además podrá obtener las direcciones IP y el uso del disco duro.
- Obtendrá información detallada sobre un único dispositivo de la red así como un resumen completo de la red, por ejemplo, el número de ordenadores con Windows que se encuentren en el departamento de marketing, o incluso la cantidad de tinta que queda en una impresora.
- Inventariar máquinas virtuales que se encuentren dentro de la red.
- Podrá administrar los números de serie de los equipos de computación.
- Registro del software instalado en la red y sus parches o actualizaciones.
- Activar alertas cuando se sobrepase el número de licencias instaladas en la red.
- Monitorear la garantía de los equipos.
- Notificaciones vía correo a los usuarios que han instalado software sin permiso.
- Informes detallados y personalizados tanto del hardware y software de los activos de computación de la compañía.

Diagrama de proceso de inventario de activos (recomendado)

Figura #3.2: Diagrama de proceso de inventario de activos (recomendado)

Elaborado por: Autores

3.2.1.2 Manual de procedimientos para el levantamiento de inventario de activos informáticos

El personal responsable de la toma de inventario de los equipos de computación deberá seguir las recomendaciones definidas en este manual de procedimiento. El jefe del departamento de TI asignará la labor y diligenciado del levantamiento de inventario de activos informáticos a una o más personas del área de sistemas. Los participantes designados para esta tarea definirán objetivos y alcances del trabajo a ejecutar.

Los activos de computación que no se encuentren inventariados por el área de TI deberán ser registrados al sistema Spiceworks y además deberán incluir los siguientes campos:

Datos del custodio. Área o departamento, se debe anotar en el recuadro correspondiente, el nombre completo del área o departamento en la cual está realizando el inventario. Nombre del responsable del equipo. Anote en el recuadro correspondiente, el nombre completo (apellidos y nombre) de la persona responsable o que hace uso de la computadora a inventariar.

Datos del equipo. Código. Anote en el recuadro correspondiente, el código de la computadora que se está inventariando, asignada por el departamento de activo fijo. Condición de operatividad. Correspondiente al estado de operatividad del dispositivo que se está inventariando tomando en consideración lo siguiente:

- Operativa en uso, si está en buenas condiciones y en funcionamiento.
- Operativa sin uso, si está en buenas condiciones pero no está siendo utilizada.
- No operativa, si no funciona debido a alguna falla o falta de recurso.

Cambiar la información del inventario de Spiceworks si la situación lo amerita, como por ejemplo: cambio de custodio, cambio de características de hardware o cambio de software. Se deberá entregar mensualmente informes acerca del ingreso de nuevos activos de información al sistema Spiceworks al jefe del área de TI y reportar cualquier movimiento o cambio al departamento de activos fijos de GNN7 TV.

3.2.1.3 Manual de usuario de Spiceworks

Acceso al sistema (Login)

Spiceworks puede ser visualizado desde cualquier equipo que pueda alcanzar el servidor. Para esto se ingresa en la URL de nuestro navegador la dirección IP o nombre de dominio del equipo seguido del puerto definido durante la instalación.

Ingresar el usuario (mail) y contraseña usados para crear su cuenta en Spiceworks. Una vez dentro encontrará el "Dashboard".

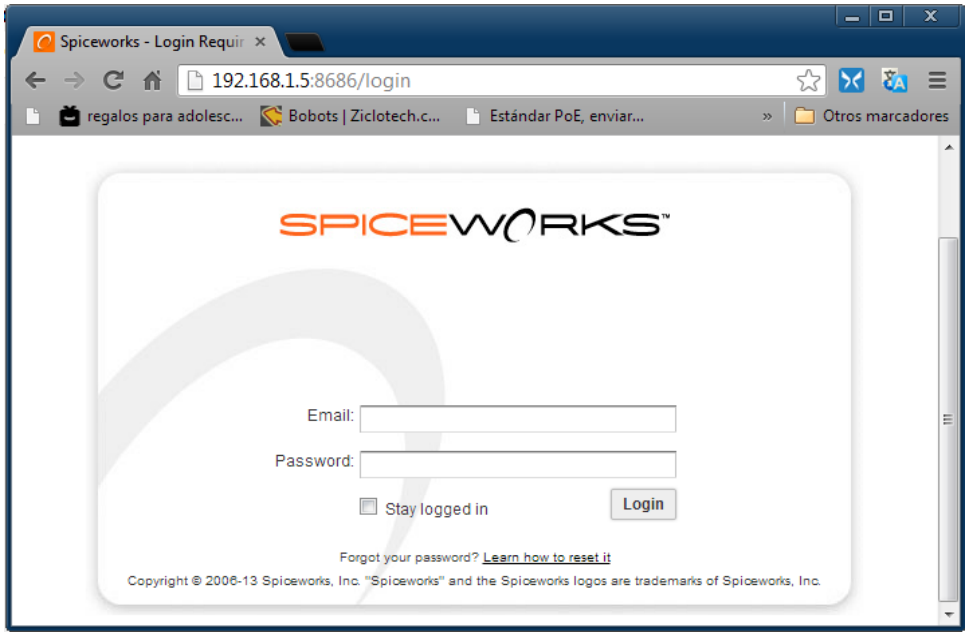


Figura #3.3: Ventana de inicio de Spiceworks

Elaborado por: Autores

Coloque el puntero sobre el menú **"**Inventory**"** y seleccione la opción de SETTINGS que se encuentran en la parte inferior izquierda.

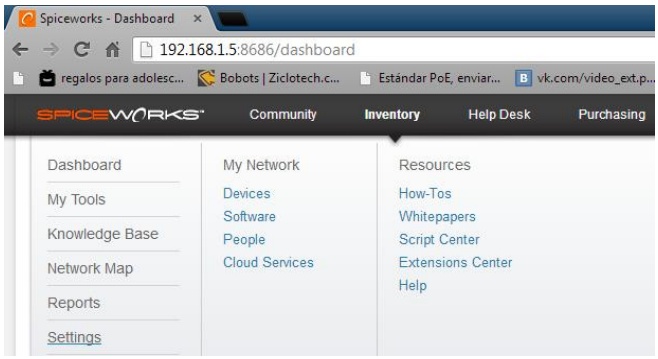


Figura #3.4: Ventana "dashboard" del Spiceworks

Elaborado por: Autores

Configuraciones

Permite desarrollar diversos aspectos del uso de Spiceworks para adaptarlo a las necesidades de GNN7 TV, por ejemplo el manejo de perfiles de escaneo para la red, los tipos de dispositivos que existirán, entre otras cosas. Es posible integrar el servidor del directorio activo a Spiceworks para simplificar la creación de los usuarios; también permite configurar alertas en base a monitoreo del sistema e instalar módulos extras con herramientas personalizaciones de Spiceworks.

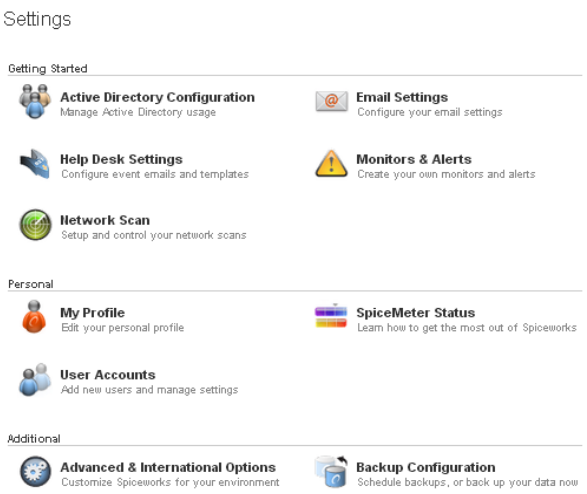


Figura #3.5: Ventana de configuraciones de Spiceworks

Elaborado por: Autores

Escaneo de la red

En la sección de "Scan Entries" se encuentran listados los diferentes escaneos que se han realizado a la red, en base al rango establecido, la fecha/hora en que se realizó, el tipo de programación que tiene y las credenciales de acceso que usa para realizar el escaneo (permisos para acceder a los equipos).

Creación de un nuevo perfil de escaneo

Para elaborar un nuevo perfil para el escaneo de la red. De clic en el enlace que dice: "Clic here to add a new scan entry".

Figura #3.6: Creando nuevo perfil de escaneo en Spicework

Elaborado por: Autores

Se mostrará una ventana emergente donde se deben ingresar los siguientes datos:

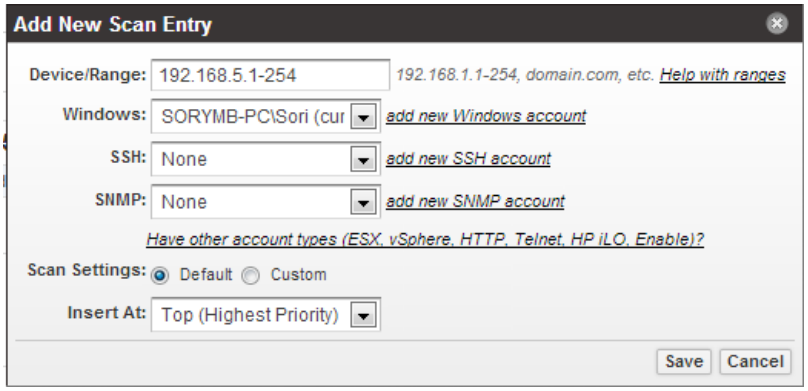


Figura #3.7: Ingresando parámetros para nuevo perfil de escaneo

Elaborado por: Autores

- **Device/Range:** Contiene una dirección IP, rango de direcciones o inclusive el nombre de dominio de un equipo.
- **Windows:** Se especifica el tipo de credenciales que se utilizarán para poder escanear los equipos con sistema operativo Windows. Generalmente la clave de administrador local de la red.
- **SSH:** Hace referencia a las claves de acceso para los equipos que manejan sistemas operativos basados en UNIX. Puede ser la del usuario "root" o de otro usuario con los permisos suficientes.
- **SNMP:** Son credenciales especiales que utiliza el "Simple Net Management Protocol". De esta forma permitirá recolectar la información necesaria de los equipos de la red que se administren bajo este protocolo.

En caso de contar con las credenciales de acceso adecuadas al momento de crear el nuevo perfil, es posible crear una con el enlace señalados en la figura anterior: "add new SSH account" o "add new SNMP account".

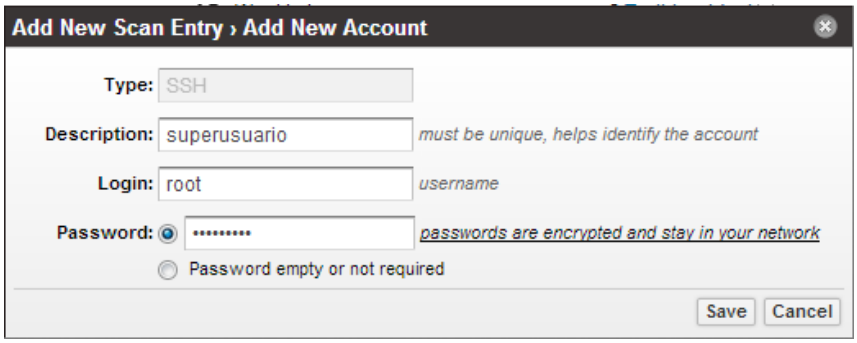


Figura #3.8: Creando nueva cuenta para escaneo

Elaborado por: Autores

En la figura anterior se muestra la creación para la clave de "root". En el cuadro "description" se ingresa un nombre representativo, en "login" el usuario con el cual se intentará acceder y en "password" la contraseña respectiva. Finalmente se procede a guardar los cambios.

- **Scan Settings:** Permite definir el tipo de programación que se le dará al escaneo, es decir si se mantendrá el horario por defecto o si se desea programar otro horario para ejecutarlo.

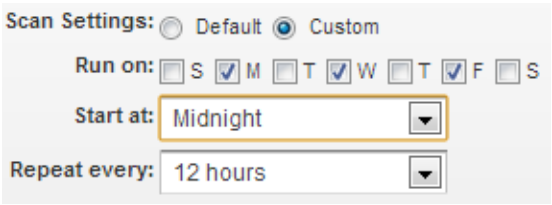


Figura #3.9: Configuración del escaneo

Elaborado por: Autores

- **Start At:** Se define la prioridad que se le va a dar al nuevo perfil de barrido que se ha creado, con respecto a los demás.

Creación de nuevas credenciales para usar en un perfil de escaneo

En la parte final de la página se encuentra la sección "Network Accounts for Scanning". Aquí se pueden editar, borrar o agregar nuevas credenciales de acceso para poder escanear los diversos equipos encontrados en la red. Por ejemplo al tratarse de un equipo Windows, se hará uso de las credenciales de administrador, mientras que para Linux/MAC podrá usarse un usuario con permisos similares a root. Para elaborar una nueva credencial, de clic sobre el enlace "Clic here to add a new network account".

Network Accounts for Scanning

Account Name	Type
Public	SNMP
SSH root	SSH
HOME-418DAD1CB0\Soraya (current user)	Windows
Click here to add a new network account	

Figura #3.10: Sección de cuentas de red para escaneos

Elaborado por: Autores

Se procede a ingresar los valores solicitados:

Figura #3.11: Ingresando parámetros para nueva cuenta de red

Elaborado por: Autores

- **Type:** Selecciona el tipo de conexión, puede ser: Windows, UNIX, Telnet, etc.
- **Description:** Se agrega un nombre descriptivo para identificarla fácilmente.
- **Login:** Ingresa el usuario que utilizará la nueva cuenta.
- **Password:** Ingresa la clave respectiva del usuario.

Modificación del horario por defecto para los perfiles de escaneo

Seleccione los días que se van a ejecutar, la hora de inicio y finalmente cada cuanto tiempo se van a realizar (máximo 1 día).

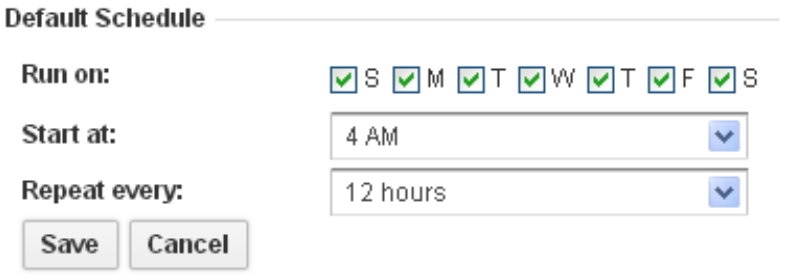


Figura #3.12: Configuraciones por defecto para escaneos programados

Elaborado por: Autores

Nota: Para la realización de perfiles de escaneo se utiliza el horario por defecto pero los mismos pueden ser programados de manera personalizada en cada uno de los perfiles.

Monitoreo y alertas

La configuración de esta sección permitirá al personal designado recibir una alerta por medio de correo electrónico ante cualquier anomalía que se detecte. Esto dependiendo de los tipos de monitoreo que se hayan programado.

Nota: Es importante notar que para recibir las alertas es necesario que estén activas ambas casillas: "Email" y "On".

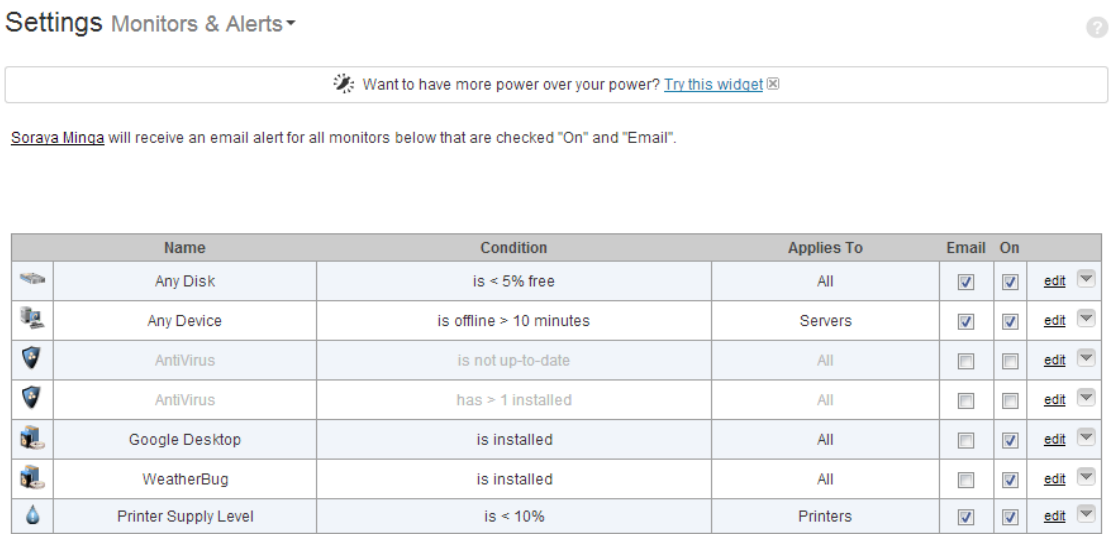


Figura #3.13: Ventana de configuración de alertas

Elaborado por: Autores

Creación de un nuevo perfil de monitoreo

Para poder crear un nuevo perfil de monitoreo, se da clic sobre el enlace: "Clic here to add a new monitor"**.** Se procede a seleccionar los parámetros necesarios según el tipo de perfil de monitoreo que se necesita.

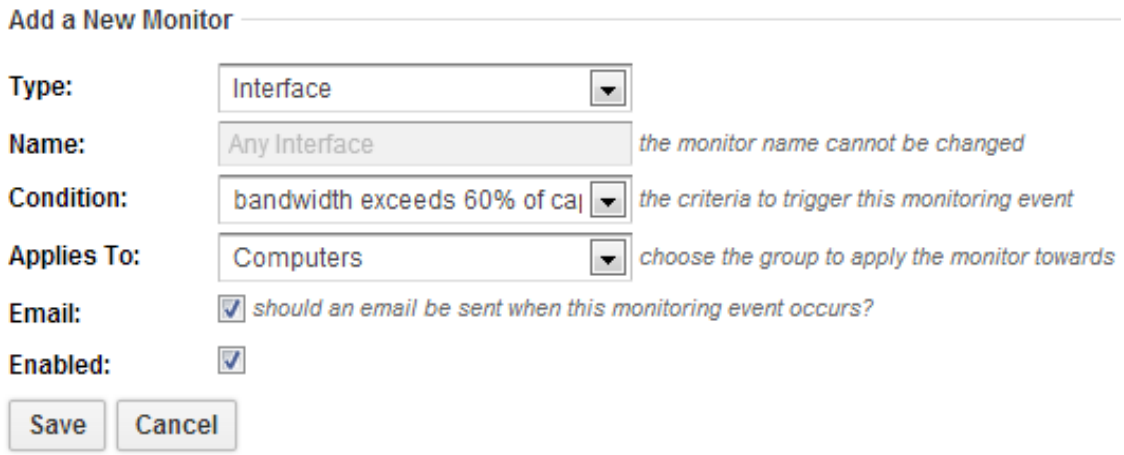


Figura #3.14: Agregando nuevo monitor

Elaborado por: Autores

- **Type**: Selecciona a que hará referencia el perfil, por ejemplo a hardware, software o algún funcionamiento del equipo en particular.
- **Condition:** Condición que deberá cumplir lo que hayamos elegido monitorear
- **Applies To:** Indica a qué tipo de equipos se aplicará el nuevo monitoreo.
- **Email:** Selecciona esta casilla en caso de que desee recibir un correo cuando algún equipo cumpla con las condiciones antes definidas.
- **Enable:** Seleccione esta casilla si desea que esté activo el monitoreo.

Opciones avanzadas e internacionales

En esta sección es posible crear atributos personalizados para los equipos, usuarios, etc. que han sido ingresados a Spiceworks, además de cambiar datos de configuración del mismo, como son el idioma, la moneda, el formato de la fecha, entre otras cosas.

Creación de nuevos atributos

En la sección de “Custom Attributtes” dar clic en el botón “Add”. Obtendrá una imagen así:

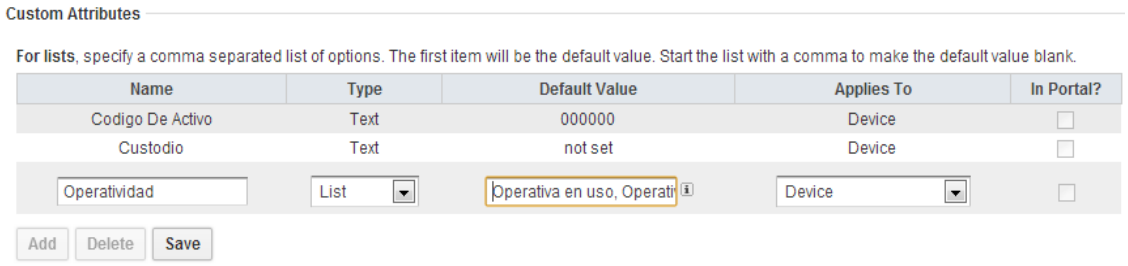


Figura #3.15: Configurando nuevos atributos

Elaborado por: Autores

- **Name:** Ingresa el nombre del nuevo atributo.
- **Type:** Define el tipo de atributo. Por ejemplo un campo de texto, una lista, etc.
- **Default Value:** Valor por defecto del nuevo campo. Puede ser en blanco o contener información.
- **Applies To:** Selecciona el tipo de elemento de Spiceworks será aplicado.

Una vez ingresados estarán disponibles para su visualización en cada uno de los dispositivos como se muestra en la siguiente figura.

Figura #3.16: Ventana donde se visualizan atributos creados

Elaborado por: Autores

Grupos personalizados

Esta sección permitirá crear grupos personalizados para separar los equipos encontrados en el escaneo o inclusive crear grupos para aquellos que no aparecen pero que de igual forma pertenecen a GNN7 TV, esto principalmente con la finalidad de tener un control sobre el inventario.

Creación de nuevos grupos para los dispositivos

Para crear un nuevo grupo debe dar clic en el botón “New Group”.

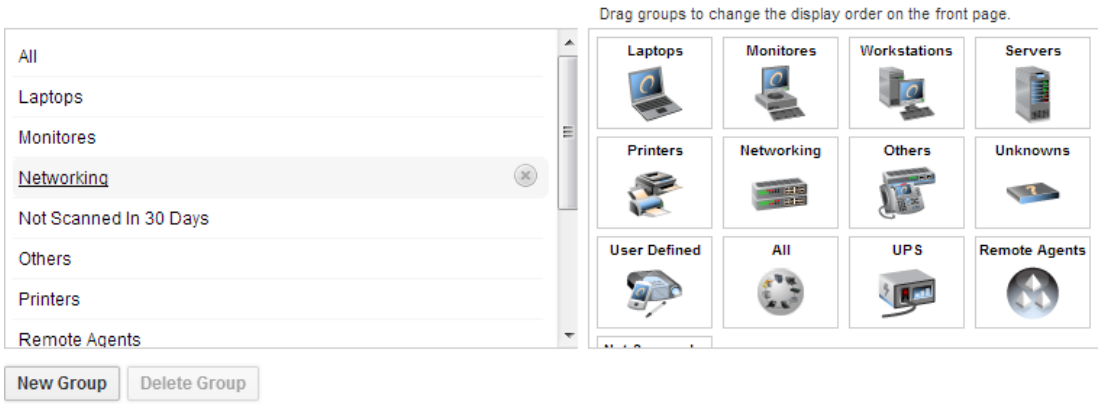


Figura #3.17: Creación de grupos para los diferentes tipos de dispositivos

Elaborado por: Autores

Posteriormente ingresa el nombre del nuevo grupo que desee crear y en caso de que desee puede cambiar el ícono que lo representará por algún otro disponible.

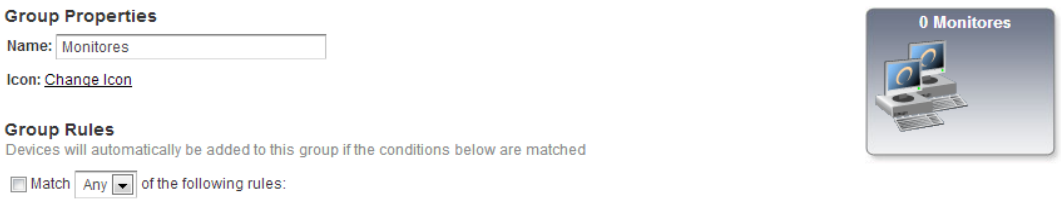


Figura #3.18: Definiendo parámetros para un nuevo grupo de dispositivos

Elaborado por: Autores

Dispositivos (Devices)

Visualización de equipos encontrados en el escaneo

Los dispositivos encontrados durante el escaneo son divididos en diferentes categorías o grupos. Para visualizarlos ingrese a la pestaña "Inventory – Devices".

Figura #3.19: Dispositivos encontrados luego de un escaneo

Elaborado por: Autores

Al ingresar a cualquiera de los grupos se obtiene un icono por cada uno de los dispositivos encontrados, con información detallada sobre el mismo, como por ejemplo: el tipo de procesador, sistema operativo, MAC, marca, modelo, etc.

Figura #3.20: Detalle de características de dispositivos inventariados en Spiceworks

Elaborado por: Autores

Ingrese a la pestaña de “Configuration” para obtener información de los componentes de hardware del equipo.

Figura #3.21: Información detallada sobre los periféricos de un dispositivo

Elaborado por: Autores

Ingrese a la pestaña **“Software”** para obtener un listado de los diversos programas o servicios que se encuentran funcionando en el dispositivo.

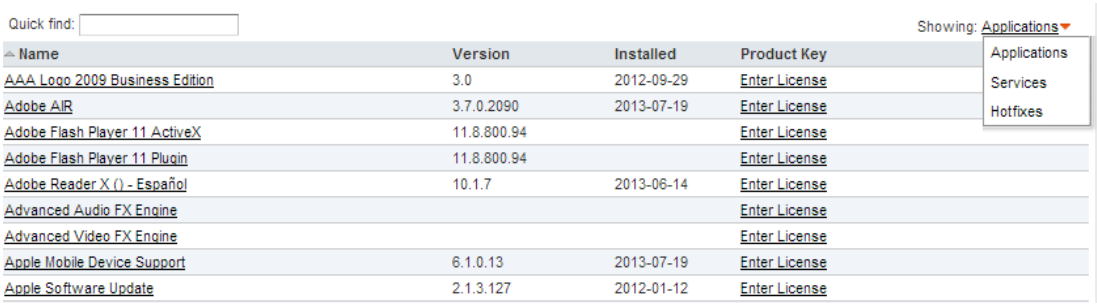


Figura #3.22: Información detallada de las aplicaciones instaladas en dispositivos

Elaborado por: Autores

Ingrese a la pestaña de **"Notes"** para agregar comentarios acerca del equipo, por ejemplo para saber si ha presentado algún tipo de anomalía, o llevar un registro de los Custodios que ha tenido el mismo.

Utilice la sección de "Tools" para realizar pruebas de monitoreo o soporte remoto como: ping, traceroute, conexión remota propia de Windows, entre muchas otras opciones.

Editar de un dispositivo/activo

Al revisar un equipo es posible modificar ciertos atributos del mismo, para esto damos click en el icono de "Editar" que se encuentra en cada uno de los equipos. De esta forma los campos se mostrarán a manera de campos de texto, listas y demás para poder ser modificados. Como por ejemplo agregar un precio y fecha de compra, el código de activo, propietario, custodio, etc. Inclusive es posible ingresar el equipo dentro de otros grupos.

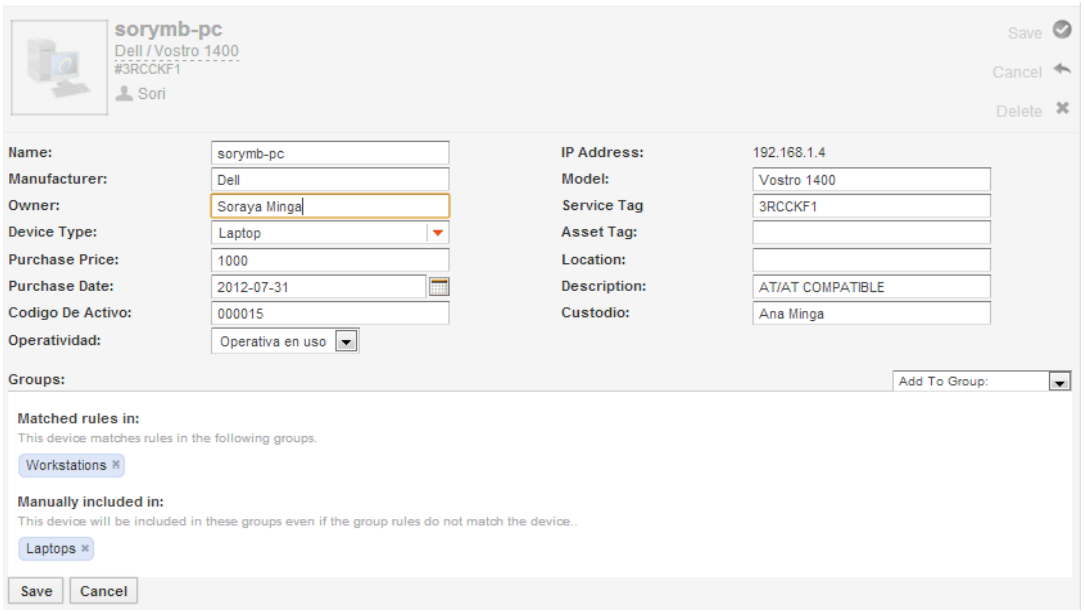


Figura #3.23: Modificando información de un dispositivo

Elaborado por: Autores

Creación de un dispositivo/activo

En la sección “Devices” dar click sobre “New Asset” y completar los parámetros.

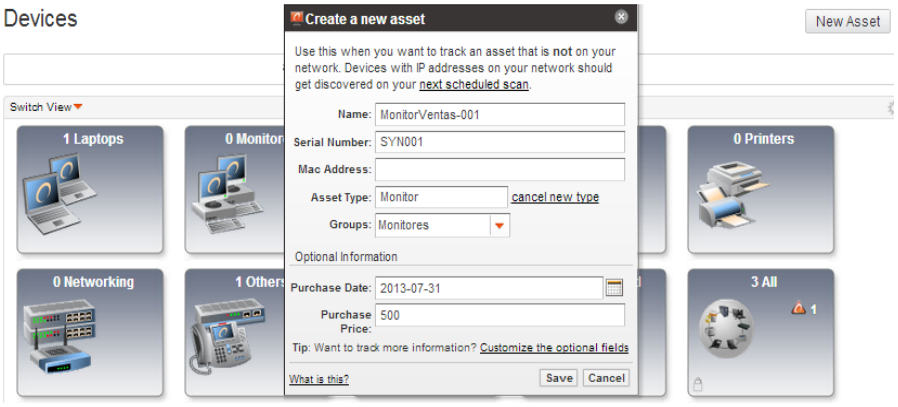


Figura #3.24: Creando nuevo dispositivo en Spiceworks

Elaborado por: Autores

Software

Para conocer todos los detalles de los programas que se encuentran instalados en la red debe ingresar a la pestaña “Invetory-Software”.

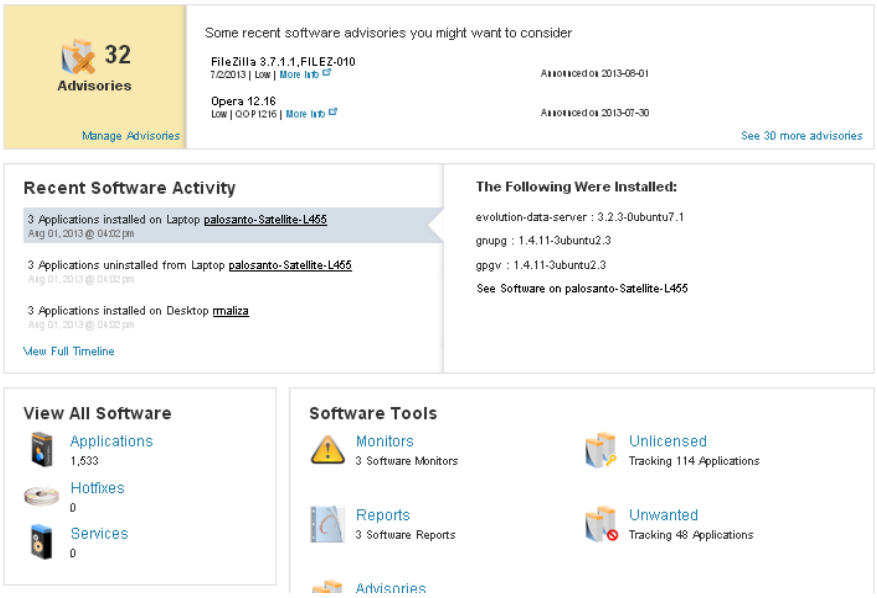
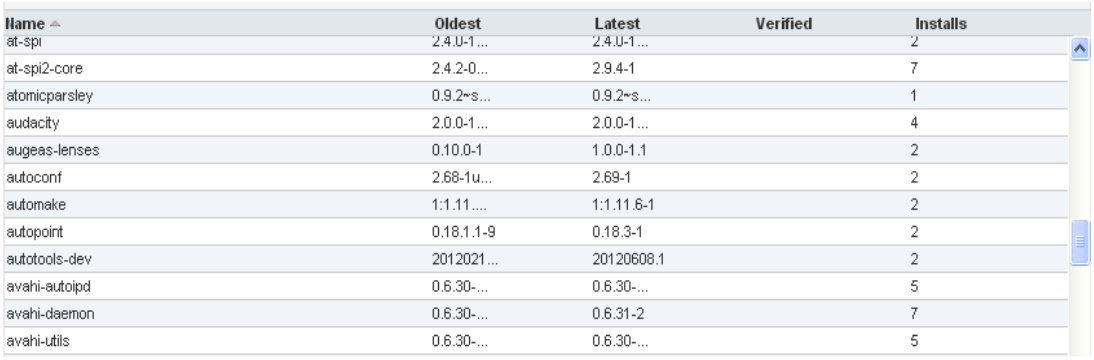


Figura #3.25: Ventana de resumen de las aplicaciones instaladas en el dispositivo

Elaborado por: Autores

Ingrese a “View All Software” para obtener un listado de las aplicaciones encontradas, sino que además es posible identificar que equipos la tienen.



Name	Oldest	Latest	Verified	Installs
at-spi	2.4.0-1...	2.4.0-1...		2
at-spi2-core	2.4.2-0...	2.9.4-1		7
atomicparsley	0.9.2~s...	0.9.2~s...		1
audacity	2.0.0-1...	2.0.0-1...		4
augeas-lenses	0.10.0-1	1.0.0-1.1		2
autoconf	2.68-1u...	2.69-1		2
automake	1:1.11....	1:1.11.6-1		2
autopoint	0.18.1.1-9	0.18.3-1		2
autotools-dev	2012021...	20120608.1		2
avahi-autoipd	0.6.30-...	0.6.30-...		5
avahi-daemon	0.6.30-...	0.6.31-2		7
avahi-utils	0.6.30-...	0.6.30-...		5

Figura #3.26: Detalle de todas las aplicaciones encontradas en un dispositivo

Elaborado por: Autores

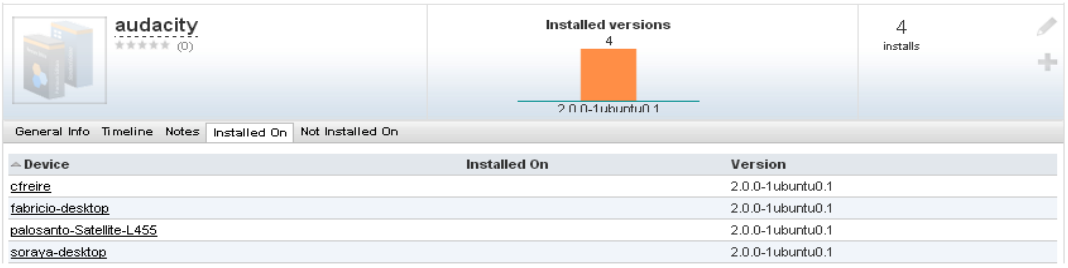


Figura #3.27: Detalles específicos de una aplicación instalada en un dispositivo

Elaborado por: Autores

Personas (People)

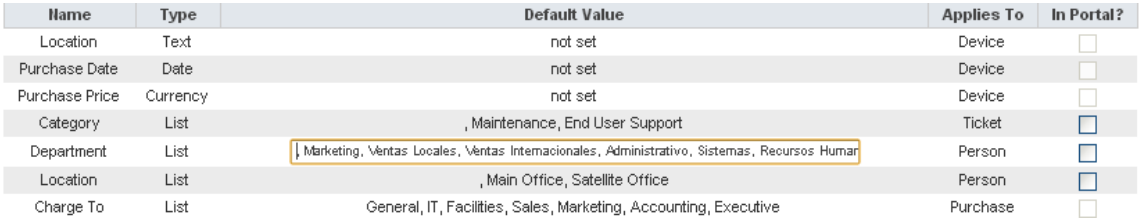
Spiceworks permite crear nuevos usuarios para el uso de la aplicación, como son los administradores y de igual forma es posible crear usuarios que representen al personal de GNN7 TV.

Figura #3.28: Ventana de creación de usuarios en Spiceworks

Elaborado por: Autores

Creación de departamentos para los usuarios

Ingrese a la sección "Inventory – Settings – Advanced & International Options"**.** En la casilla "Standard Atributes" se modifica el campo llamado "Department".



Name	Type	Default Value	Applies To	In Portal?
Location	Text	not set	Device	☐
Purchase Date	Date	not set	Device	☐
Purchase Price	Currency	not set	Device	☐
Category	List	, Maintenance, End User Support	Ticket	☐
Department	List	, Marketing, Ventas Locales, Ventas Internacionales, Administrativo, Sistemas, Recursos Humar	Person	☐
Location	List	, Main Office, Satellite Office	Person	☐
Charge To	List	General, IT, Facilities, Sales, Marketing, Accounting, Executive	Purchase	☐

Figura #3.29: Creación de grupos de usuarios en Spiceworks

Elaborado por: Autores

Creación de usuarios

Una vez que tenemos definidos los departamentos necesarios, se puede iniciar con la creación de los usuarios que representan al personal que labora en GNN7 TV. Para esto damos click en "New Person" y procedemos a llenar los campos solicitados.

Figura #3.30: Ingresando parámetros para la creación de usuarios

Elaborado por: Autores

Guardados los cambios, se ingresará a la página del departamento al cual has agregado a la nueva persona y se mostrará la información del mismo.

Añadir equipo a usuario

Para agregar un dispositivo al nuevo usuario o editar algunas de sus campos debe dar click en el botón "Editar". En el campo "Add Device"**,** se escribe el nombre del equipo que se desea añadir a la persona. Es posible tener más de un equipo asignado.

Figura #3.31: Ventana con información detallada de un usuario

Elaborado por: Autores

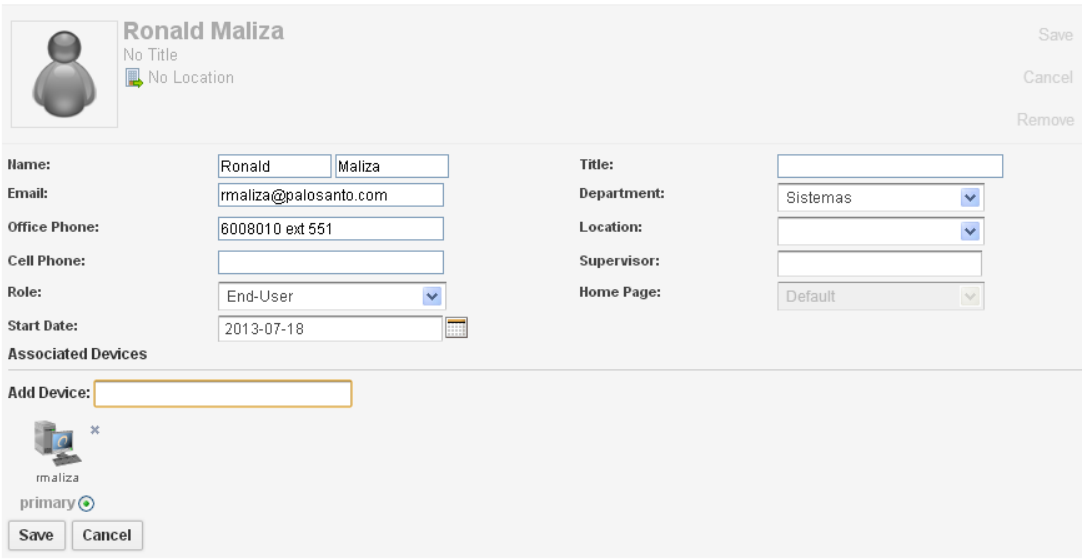


Figura #3.32: Asignando dispositivos a los usuarios en Spiceworks

Elaborado por: Autores

Reportes

Spiceworks ofrece ciertos reportes por defecto, por ejemplo para saber el espacio en disco o de las aplicaciones que se encuentran instaladas, entre otros. Esto se encuentra en la sección "Inventory – Reportes"

Ejecución/Edición de un reporte

Para ejecutar un reporte debe dar click sobre el enlace ubicado del lado derecho de cada uno de ellos: “run”. En este mismo vínculo se encuentra la opción de editar el mismo, para esto da click en “edit”. Es posible exportar el resultado en formato CSV, Excel o PDF dando click sobre el botón “Export”.

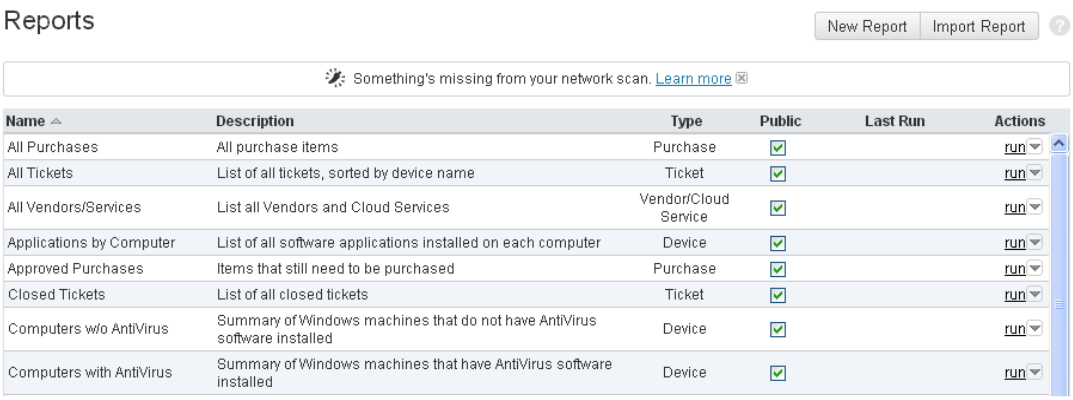


Figura #3.33: Ventana donde están listados todos los reportes de Spiceworks

Elaborado por: Autores

Instalación de reportes de terceros

En la parte final de “Inventory - Reports” se encuentra una sección donde se ubican reportes que han sido compartidos por otros usuarios de Spiceworks. Para hacer uso de ellos da click en “Install” y autenticarse como usuario de la comunidad Spiceworks**.**

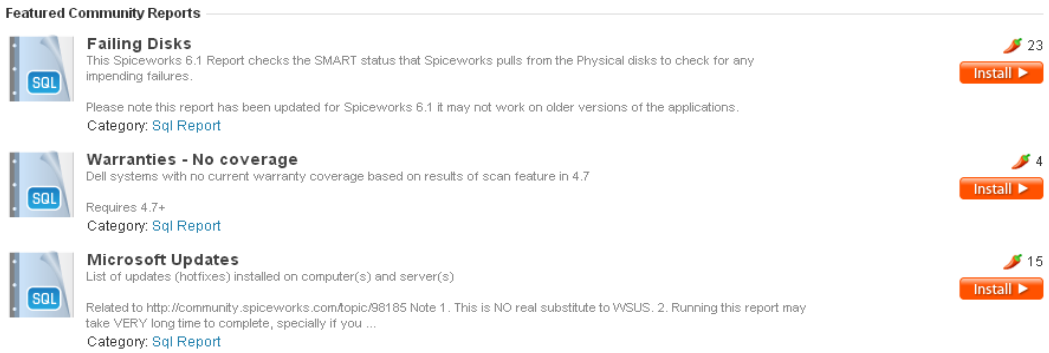


Figura #3.34: Instalando nuevos reportes en Spiceworks

Elaborado por: Autores

Creación de reportes

Para crear un nuevo reporte debe dar click en el botón “New Report”. Y se completan los datos necesarios. En la sección “What to include in report” se especifica sobre que se va a trabajar: dispositivos, personas, tickets, etc. Dependiendo de eso aparecerán los campos respectivos en “Columns to display”.

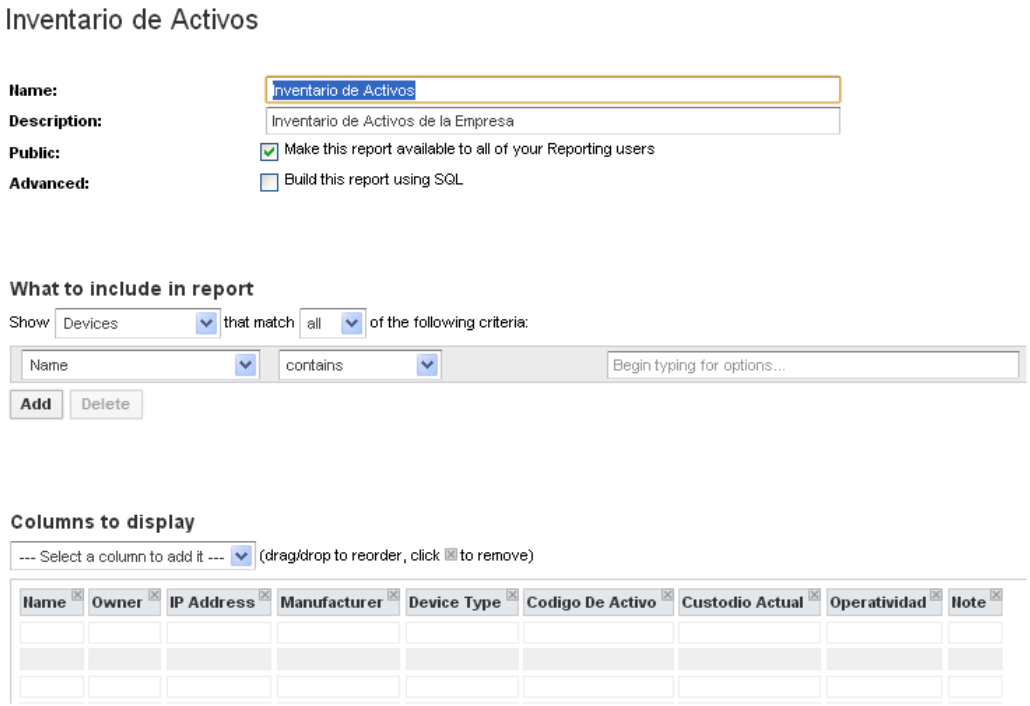


Figura #3.35: Creación de reportes en Spiceworks

Elaborado por: Autores

Al generar el reporte se obtiene un resultado similar al siguiente:

PS: Inventario de Activos

Inventario de Activos de la Empresa (19 items)

Generated on Aug 01, 2013 @ 09:27 pm

Name	Owner	IP Address	Manufacturer	Device Type	Codigo De Activo	Custodio Actual	Operatividad	Note
192.168.1.14	Luis Andino	192.168.1.14	Xiamen Yealink Net Tech Co	VoIP Device	00020	Luis Andino	Operativo en uso	2013-04-30 - Aquisición del equipo 2013-05-01 - Teléfono entregado a Luis Andino
192.168.1.28		192.168.1.28	D-link	HTTP Device	00031	Ronald Maliza	Operativo sin uso	
192.168.5.11	Mario Torres	192.168.5.11	Aastra	VoIP Device	000001	Miguel Garrido	Operativo sin uso	2013-07-01 - Teléfono entregado a Mario Torres para su uso 2013-08-01 - Teléfono entrgado a Miguel Garrido para revisión

Figura #3.36: Ventana con resultados obtenidos por un reporte de Spiceworks

Elaborado por: Autores

Solución de problemas para dispositivos

En ocasiones se reconocen equipos pero los mismos quedan en un estado indefinido, mostrando una alerta. Esto puede ser debido a que las credenciales que hemos ingresado no son las correctas para poder acceder.

Problemas de credenciales (Accounts)

Estos equipos aparecen bajo del grupo de "Unknowns". Para resolver esto, se debe ingresar a cada uno de ellos y probar con credenciales diferentes en base al tipo de equipo que sea. Se muestran de manera similar a la siguiente:

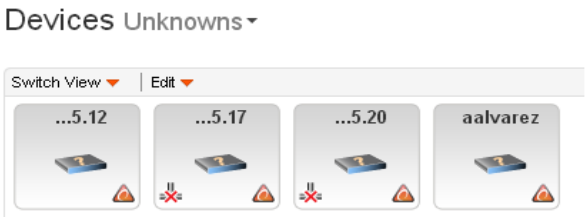


Figura #3.37: Ventana de dispositivos inventariados pero con poca información

Elaborado por: Autores

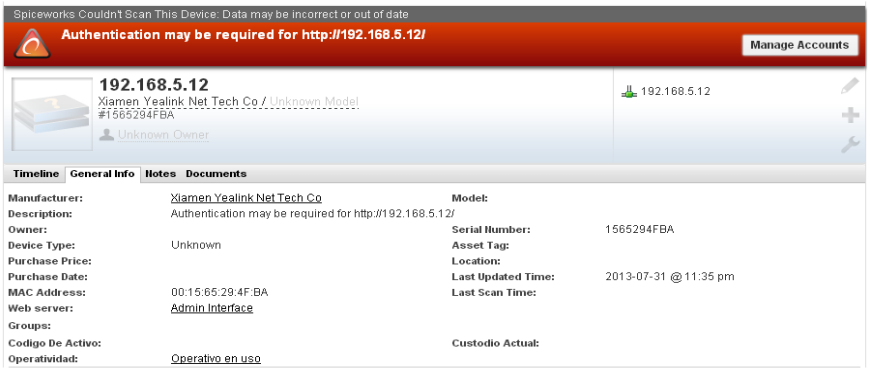


Figura #3.38: Ventana con resumen de dispositivo desconocido

Elaborado por: Autores

Da click en "Manage Accounts" y creamos una nueva con las credenciales antes mencionadas.

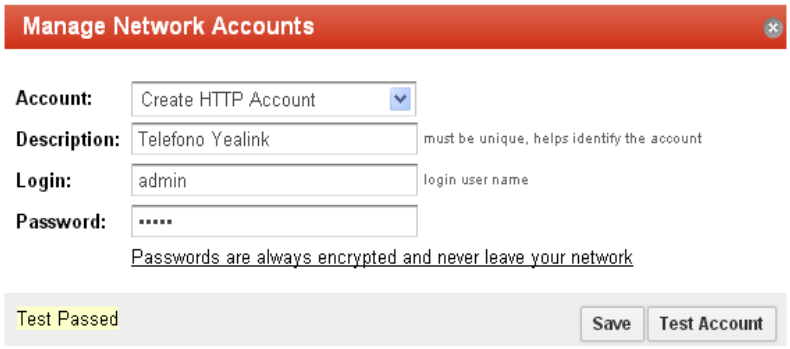


Figura #3.39: Creando nuevas credenciales para dispositivos

Elaborado por: Autores

3.2.1.4 Formatos y Plantillas

FORMATO INVENTARIO DE COMPUTADORAS Y SOFTWARE BÁSICO																
DATOS CUSTODIO		DATOS COMPUTADORA				DATOS DEL PROCESADOR			DATOS DEL BIOS		DATOS DEL S.O.	DATOS DEL SOFTWARE BÁSICO				
Departamento	Nombre	Código	Marca	Modelo	Condición de Operatividad	Fabricante	Tipo	Velocidad	Fabricante	Fecha de Fabricación	Sistema Operativo	Nombre	Versión	Fabricante	Idioma	Licencia

Figura #3.40: Formato de inventario de computadoras y software básico

Elaborado por: Autores

FORMATO INVENTARIO DE HARDWARE (Equipos de Escritorio)																				
USUARIO		CPU									MONITOR						ACCESORIOS			
Nombre	Departamento	S/N	OEM	Modelo	Procesador	RAM	Disco Duro	MAC Address	Fecha de Compra	Costo (dólares)	OEM	Modelo	Tamaño	Tipo	Fecha de Compra	Costo (dólares)	Mouse	Webcam	Parlantes	Micrófono

Figura #3.41: Formato de inventario de computadoras de escritorio

Elaborado por: Autores

FORMATO INVENTARIO DE SERVIDORES Y SOFTWARE BÁSICO																
DATOS CUSTODIO		DATOS COMPUTADORA				DATOS DEL PROCESADOR			DATOS DEL BIOS		DATOS DEL S.O.	DATOS DEL SOFTWARE BÁSICO				
Departamento	Nombre	Código	Marca	Modelo	Condición de Operatividad	Fabricante	Tipo	Velocidad	Fabricante	Fecha de Fabricación	Sistema Operativo	Nombre	Versión	Fabricante	Idioma	Licencia

Figura #3.42: Formato de inventario de servidores y software básico

Elaborado por: Autores

FORMATO INVENTARIO DE IMPRESORAS															
DEPARTAMENTO		FABRICANTE				HARDWARE						EMPRESA			
Nombre	No. Usuarios	OEM	Tipo	Modelo	S/N	Velocidad de Impresión	Resolución	Tamaño del Buffer	Interfaz de Conexión	Formato de Papel	MAC Address	S/N	Fecha de Compra	Costo (dólares)	Estado

Figura #3.43: Formato de inventario de impresoras

Elaborado por: Autores

FORMATO INVENTARIO DE EQUIPOS DE RED																	
HOSTNAME	FABRICANTE				HARDWARE										EMPRESA		
Nombre	OEM	Modelo	Tipo	S/N	Estandar	Max. VLANs	Velocidad CPU	Memoria	Interfaces Seriales	Conectores RJ-11	Conectores RJ-45	Dimensiones (mm.)	Power input	Entorno de Trabajo	S/N	Fecha de Compra	Costo (dólares)

Figura #3.44: Formato de inventario de equipos de red

Elaborado por: Autores

3.2.1.5 Auditoria - Propiedad de los activos

Objetivo

El objetivo de este control es que toda la información y activos asociados para su tratamiento deben estar registrados y asignados a una persona o parte designada de la organización.

Alcance

El alcance de este control es que el personal o las áreas dentro de GNN7 TV asuman la responsabilidad sobre todo evento asociado a los distintos activos informáticos de su propiedad. Este documento muestra los puntos a tomar en cuenta al momento de asignar responsabilidades, los más importantes son:

- Los derechos, responsabilidades y obligaciones de los usuarios sobre los recursos informáticos que le sean asignados.
- Las condiciones iniciales de un activo y el buen uso que este le debe dar.

Auditoría

La asignación de activos de información actualmente no cuenta con una correcta gestión, esto conlleva a que los miembros de la organización no conozcan sus responsabilidades y obligaciones sobre los mismos.

El departamento de TI no ejecuta el adecuado proceso para la asignación de los activos de información, esto conlleva a que los miembros de la organización desconozcan sus obligaciones y responsabilidades.

El proceso de asignación se ejecuta de la siguiente manera:

- Ingreso del activo de información al departamento de TI.
- Configuración e instalación de aplicaciones según los requerimientos necesarios.
- Coordinar con el usuario la entrega del activo de información.
- Entregar el activo de información al usuario.

En este proceso se pudieron detectar las siguientes falencias:

- Luego de asignar un activo de información a un miembro de la organización, no se registra la propiedad dentro del inventario de activos (Control 3.2.1.1)
- No se firma ningún documento que indique que el usuario está de acuerdo y acepta sus responsabilidades y obligaciones sobre los activos que le fueron asignados.
- Para el caso de la reasignación de activos de información, no existe un historial de propiedad.

Diagrama de proceso de propiedad de los activos (Actual)

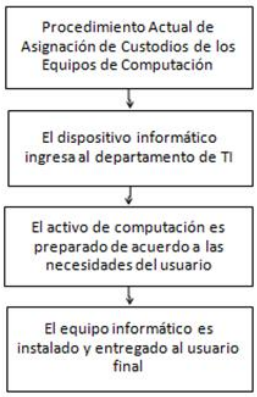


Figura #3.45: Diagrama de proceso de propiedad de los activos (actual)

Nota: Información obtenida del Jefe del departamento de TI de GNN7 TV, elaborado por: Autores

Recomendaciones

En esta parte del documento se detallarán recomendaciones para mejorar el proceso actual de asignación de activos de información:

- Definir los diferentes grupos o usuarios según su tipo de vinculación.
- Será responsabilidad del departamento de TI los equipos computacionales recibidos físicamente, hasta el momento en que el bien sea entregado por medio de la salida del departamento y registrado debidamente en un formulario.
- Los activos ingresados no podrán salir del área, sin que el personal no haya realizado la gestión respectiva de inicialización, instalación de programas y actualizaciones generales del equipo de computación para que sea entregado al custodio y éste pueda tener uso efectivo del mismo.
- La vinculación de una persona con GNN7 TV debe ser registrada en la base de datos del área de TI en el caso de que utilicen algún activo informático.
- Las condiciones de uso de los dispositivos informáticos pueden variar en función de las necesidades de GNN7 TV, del departamento al que pertenece el usuario o de nuevos controles que implemente el área de sistemas.

- Los jefes de área en conjunto con el jefe del departamento de TI deberán decidir qué recursos serán asignados a cada persona y validar las condiciones en que estos fueron entregados.

- Definir la responsabilidad y obligaciones de los miembros de la organización sobre los activos de información y plasmarlas en un acta de responsabilidad de los activos (Ver anexo #1). El formato establecido para dicha contendrá los siguientes campos: nombre del departamento responsable, nombre del jefe de área, nombre del custodio responsable, fecha de entrega del activo, descripción del activo, código del activo, firma del custodio responsable del activo, firma del jefe de área, y firma del responsable de TI.

- El acta de responsabilidad (Anexo #1) debe ser aceptada por el custodio y responsables de los activos (jefe del departamento de TI y jefe de área).

- Hacer conocer las políticas sobre el buen uso de los activos de información (Control 3.2.1.7) a todos los miembros de la organización.

- El personal de TI debe realizar inspecciones periódicas a los puestos de trabajo y a los activos para verificar que se cumpla con el acuerdo de propiedad de los activos y se dé un buen uso a los mismos.

- Dentro del acuerdo de responsabilidad se debe incluir que el custodio debe cumplir la normativa general y comunicar al responsable administrativo o responsable de TI sobre cualquier anomalía detectada en el uso o en el funcionamiento del recurso informático.

- El personal de TI debe gestionar los préstamos y salidas de activos de información, además deberá registrar en el formulario "Registro de salida y/o préstamo de activos fijos computacionales" (Anexo #2).

- La solicitud de "Salida y/o préstamo de activos fijos computacionales" constará de toda la información relacionada a la transferencia y deberá estar firmada por las personas que la autorizan.

- Únicamente el personal de la institución, podrá tener bajo su custodia equipos adquiridos por la organización.

Diagrama de proceso de propiedad de los activos (recomendado)

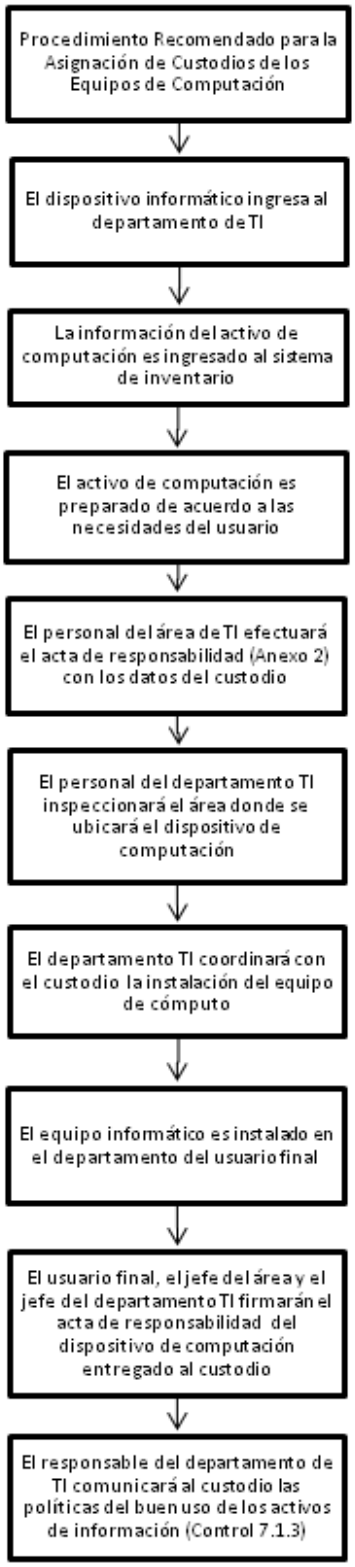


Figura #3.46: Diagrama de proceso de propiedad de los activos (recomendado)

Elaborado por: Autores

3.2.1.6 Procedimiento para la asignación de activos de información

- El personal responsable de gestionar la asignación de activos deberá seguir las recomendaciones definidas en este procedimiento.

- El jefe del departamento de TI designará al personal responsable de gestionar la asignación de activos de información.

- La persona designada deberá llevar el control registrando los activos asignados (Ver 3.2.1.2).

- La persona designada gestionará la entrega del acta de responsabilidad de activos al usuario final y a su vez explicar en qué consiste la responsabilidad sobre los mismos (Ver 3.2.1.3).

- Periódicamente el encargado responsable de la gestión de asignación de activos deberá presentar al jefe del departamento de TI y al área de activos fijos de la organización un informe detallando los cambios o asignaciones registrados mensual o semanalmente.

- Los activos ingresados no podrán salir del área, sin que el personal de sistema realice la gestión respectiva de inicialización, instalación de programas y actualizaciones generales del equipo de computación para que sea entregado al custodio y éste pueda tener uso efectivo del mismo.

- El departamento de TI tendrá a su cargo la entrega y posesión de los activos fijos registrados a través del formulario "Acta de responsabilidad sobre los activos" (Ver anexo #1) que firmará el usuario final, conservando una copia del mismo en el cual irá detallado datos de la fecha de entrega de activo así como el estado y desglose de lo que se entrega con los respectivos códigos de asignación.

- Se deberá coordinar la entrega e instalación del equipo de computación y verificar que el área de ubicación cumpla con los requisitos mínimos para el funcionamiento óptimo y buen desempeño del activo, los cuales son: seguridad física, las condiciones ambientales, la alimentación eléctrica y acceso adecuado.

- Cumplidos los requisitos previos, el personal del departamento de TI le comunicará al custodio vía correo electrónico la fecha de entrega e instalación del equipo o accesorio de computación. El usuario deberá aceptar dicha comunicación a través de la misma vía.

- Será responsabilidad del usuario final la custodia de los activos de computación asignados; en caso de extravío o robo, se sujetará a lo establecido en la "Política de reutilización y retirada segura de los equipos de computación".

- Todo movimiento de activo fijo computacional que implique una salida de las instalaciones de oficinas y/o préstamo a los usuarios, deberá efectuarse mediante un formulario (Anexo #2) que firmará el solicitante.

3.2.1.7 Auditoria - Uso aceptable de los activos

Objetivo

El objetivo de este control es identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados al tratamiento de la misma dentro de la organización.

Alcance

El alcance de este control es establecer políticas para el buen uso de todos los activos informáticos y servicios tecnológicos de GNN7 TV, con el fin de optimizar recursos y dar un correcto tratamiento a la información.

Auditoria

GNN7 TV actualmente cuenta con un solo documento llamado: "Manual de políticas y procedimientos: Políticas de seguridad informática", donde agrupa políticas generales sobre el uso aceptable de los activos y recursos tecnológicos de GNN7 TV; la consecuencia de no contar con políticas específicas es que el departamento de TI no puede implementar controles óptimos para velar por el buen uso de los mismos.

Recomendaciones

Se recomienda reemplazar el "Manual de políticas y procedimientos: Políticas de seguridad informática" por reglamentos específicos para cada recurso tecnológico otorgado por GNN7 TV, a continuación se detallan las normas con mayor prioridad para la organización:

- **Política general del uso aceptable de los activos**. Esta norma específica las metas e iniciativas a cumplir para administrar de manera responsable y eficiente los equipos informáticos y poder mantener la confidencialidad, integridad y disponibilidad de los diferentes sistemas de información (Ver 3.2.1.8).

- **Política para el uso correcto del correo electrónico.** Esta política administrativa establece el uso, acceso y divulgación de correo electrónico además ayudará a garantizar que los recursos de GNN7 TV sirvan para esos propósitos (Ver 3.2.1.9).

- **Política del uso aceptable del internet.** Esta política tiene por objeto ayudar a mejorar el uso de los recursos de Internet que se encuentran a disposición de los empleados (Ver 3.2.1.10).

- **Política para cambios o reubicaciones.** El propósito de esta política es establecer un enfoque para el control de cambios técnicos de los activos informáticos de GNN7 TV (Ver 3.2.1.11).

- **Política para la comunicación inalámbrica "Wireless".** Esta política establece las condiciones que los dispositivos de infraestructura inalámbrica deberán cumplir al conectarse a la red corporativa (Ver 3.2.1.12).

- **Política de conciencia y formación para la seguridad de la información.** Esta política ayudará al departamento de TI a ejecutar programas de concienciación de seguridad de la información (Ver 3.2.1.13).

3.2.1.8 Política general del uso aceptable de los activos

El objetivo de esta política es establecer políticas para el uso aceptable de los activos informáticos y recursos de red de GNN7 TV. Todos los empleados, contratistas, consultores, trabajadores temporales de GNN7 TV, incluyendo a todo el personal afiliado con terceros están obligados a cumplir con esta política. Esta norma se aplica a los activos de información propietarios o arrendados por GNN7 TV o dispositivos que se conecten a la red de la organización o se encuentran dentro de las instalaciones.

Política general

- Todo miembro de la organización debe ejercer el buen juicio con respecto al uso apropiado de los recursos informáticos de acuerdo con las políticas, normas y directrices de GNN7 TV. Los recursos de GNN7 TV no se usarán para ningún propósito ilegal o prohibido.
- Todos y cada uno de los equipos informáticos serán asignados a un responsable, por lo que será de su competencia hacer buen uso de los mismos.
- El custodio deberá hacer cumplir a cabalidad el buen uso del computador cuando otro usuario se encuentre haciendo uso de dicho equipo.
- Los custodios de los equipos de cómputo son responsables del uso que los practicantes puedan hacer de ellos.
- Por razones de seguridad y mantenimiento, el personal del departamento de TI debe monitorear y auditar equipos, sistemas y tráfico de red.
- Los dispositivos o usuarios no autorizados que accedan a la red corporativa serán desconectados.
- La seguridad de la información prohíbe activamente bloqueos autorizados de exploraciones de auditoría.
- El firewall y otras tecnologías de bloqueo deberán permitir el acceso a las fuentes de análisis.

Acceso y uso de los recursos

El acceso a los recursos informáticos de GNN7 TV puede darse de distintos modos:

- Acceso al espacio físico (oficina, sala de cómputo, zona de cobertura inalámbrica) en donde se encuentra el recurso (ordenador personal, servidor, punto de red, punto de acceso inalámbrico).
- A través de una cuenta de acceso de GNN7 TV.

GNN7 TV se reserva el derecho de decidir el modo de acceso a sus recursos, así como la posibilidad de adoptar nuevas modalidades o suprimir otras. El modo en que se accede a un recurso de GNN7 TV está recogido en la normativa específica de uso.

Acceso al espacio físico

Para acceder a determinados recursos de GNN7 TV (ordenadores personales, servidores, puntos de red) hay que tener acceso al espacio físico en el que se encuentran, ya sea restringido o abierto. En cualquier caso, es tarea del responsable administrativo pertinente controlar quién accede al espacio físico.

Limitaciones de uso

GNN7 TV, a través de la gerencia general y el departamento de TI, podrá establecer límites en el acceso o uso de sus servicios y recursos por una de las siguientes causas:

- Mantener la operatividad y disponibilidad de los servicios y recursos.
- Garantizar el cumplimiento de la ley, por ejemplo, propiedad intelectual.
- Evitar perjuicios a sus usuarios, por ejemplo, limitando la recepción de mensajes con virus, spam, etc.

El área de TI podrá limitar o denegar el acceso a un determinado servicio o recurso cuando se detecte el uso incorrecto o no aceptable del mismo, ya se trate de un uso intencionado o provocado por alguna otra causa como daños o código malicioso.

Compromiso de confidencialidad con relación a los servicios de GNN7 TV

Todo el personal vinculado a GNN7 TV, independientemente del tipo de contrato e incluyendo aquel perteneciente a empresas externas con las que se ha establecido alguna relación contractual, asume un "compromiso explícito de confidencialidad" por el que debe cumplir con la obligación de secreto y confidencialidad respecto a los archivos y los contenidos a los que por su trabajo tenga acceso.

Excepción de responsabilidad en administración, funcionamiento y uso de servicios

El usuario acepta que el departamento de TI no tiene responsabilidad u obligación legal por pérdidas de datos, errores en las comunicaciones, o cualquier otro daño o perjuicio, cuando éstos se deriven de acciones efectuadas durante las tareas de mantenimiento de los servicios, durante situaciones especiales o emergencias provocadas por el usuario.

El área de TI queda exento de cualquier responsabilidad derivada del mal funcionamiento de los servicios que tenga su origen en una circunstancia accidental, trabajos necesarios de mantenimiento o cualquier otra causa no imputable a la misma.

Estadísticas de uso de los servicios

El departamento de TI podrá generar estadísticas del uso de servicios o recursos con el fin de medir y optimizar el rendimiento, la utilización que se hace de los mismos y detectar posibles comportamientos anómalos que pudieran producirse. En función de la legalidad vigente, queda a criterio del área de TI y de las áreas de quienes depende, qué estadísticas podrán hacerse públicas para información y mejora del servicio.

Gestión de incidencias

- Todos los usuarios están obligados a informar al departamento de TI, a través de los medios habilitados para tal efecto, sobre posibles incidencias detectadas en el funcionamiento de los servicios ofertados o uso indebido de los recursos.
- Las incidencias que afecten a un usuario concreto deben ser informadas y gestionadas por el área de TI. El compromiso del área de TI es atender cualquier incidencia con prontitud y a darle solución en el plazo más breve posible.

Sobre el uso de las infraestructuras

- La conexión de equipos de red activos (switch, access point, router) que perturbe el correcto funcionamiento de la red de GNN7 TV o comprometa la seguridad, salvo expresa autorización del departamento de TI.
- Proporcionar acceso externo desde la propia red de comunicaciones, mediante la instalación de dispositivos de acceso remoto.
- El alojamiento de dominios distintos a los usados por GNN7 TV, salvo expresa autorización de la gerencia competente en esta materia.
- La instalación de servidores telemáticos o de otro tipo (web, correo, etc.), debe respetar las medidas de seguridad adecuadas.
- La conexión, desconexión o reubicación de equipos ajenos a la organización sin la expresa autorización de los responsables de los mismos.
- No hacer un uso racional, eficiente y considerado de los recursos disponibles, tales como: el espacio en disco, la memoria, las líneas telefónicas, terminales, canales de comunicación, etc.
- Por último, también se considera hacer uso incorrecto, actuar de forma contraria a las condiciones y políticas de utilización de los servicios y recursos informáticos proporcionados por GNN7 TV, referenciados en este documento.

Activos informáticos

- Usted es responsable de la protección de los activos asignados por GNN7 TV.
- Los usuarios pueden escuchar música, siempre que esto no interfiera con su trabajo y no cause molestias a terceros u otros compañeros de trabajo.
- Todos los PCs, ordenadores portátiles y estaciones de trabajos deben asegurarse con un protector de pantalla protegido por contraseña con la función de activación automática de 10 minutos o menos. Debe bloquear la pantalla o cerrar sesión cuando el dispositivo esté desatendido.
- El único autorizado para instalar/desinstalar software es el departamento de TI, ningún usuario común o tercero puede realizar dicha acción si no es bajo la autorización y supervisión del mismo.

Cuentas del sistema

- Los usuarios son responsables de la seguridad de la información, cuentas de acceso y sistemas bajo su control.
- Mantenga contraseñas seguras y no comparta información de la cuenta o contraseñas con nadie, incluyendo a otros miembros del personal, familiares o amigos. Facilitar el acceso a otro individuo, ya sea deliberadamente o por imposibilidad, es una violación grave de esta política.
- Se debe establecer a nivel de sistemas y nivel de usuario contraseñas que vayan de acuerdo con la "Política de contraseñas".
- Asegurarse mediante medios jurídicos y técnicos la propiedad de la información confidencial que se encuentra bajo el control de GNN7 TV. Los negocios que almacenan información privada sobre el personal o ambientes no contralados por GNN7 TV, incluidos los dispositivos mantenidos por terceros con quien la empresa no tiene un acuerdo contractual, están prohibidas. Está prohibido el uso de cuentas de correo electrónico que no hayan sido proporcionado por el departamento de TI o por sus clientes y socios.

Medios extraíbles

Se prohíbe el uso de memorias USB personales, en caso de que se requiera por motivos de trabajo, deberá ser solicitada su compra a administración, con el objetivo de su uso sea exclusivamente interno. En caso de que una memoria USB propiedad de GNN7 TV sea utilizada en un computador externo a GNN7 TV, previo a su uso en cualquier computador de GNN7 TV, deberá ser enviado para su revisión al departamento de TI. En caso de que por horario o urgencia no sea posible, debe ser reportado de inmediato al área de TI.

Uso de la red

Usted es responsable de la seguridad y uso apropiado de los recursos de red corporativa bajo su control. Se encuentra estrictamente prohibido el uso indebido de los recursos de GNN7 TV para los siguientes casos:

- Provocar fallos de seguridad en la organización o en los recursos de red, incluyendo el acceso a datos, servidores o cuentas a los cuales no están autorizados; eludir la autenticación de usuario en cualquier dispositivo o efectuar "sniffing" al tráfico de red.
- La introducción de honeypots, honeynets, o tecnología similar a la red de GNN7 TV.
- Causar una interrupción del servicio en GNN7 TV o de algún otro recurso de red, incluyendo inundaciones ICMP (ICMP floods), suplantación de paquetes (packet spoofing), denegación de servicio, desbordamiento de montículo o buffer (heap or buffer overflows), y falsificado la información de enrutamiento con fines maliciosos.
- La violación de las leyes de copyright, incluyendo el duplicar o transmitir imágenes con derecho de autor, música, video y software.
- El uso del Internet o de la red corporativa que viole la "Política del uso aceptable del Internet".

- Introducir intencionalmente código malicioso, incluyendo los virus, gusanos, troyanos, email bombs, spyware, adware y keyloggers.

- Escaneo de puertos o análisis de seguridad en la red de producción que no haya sido autorizada previamente por el departamento de TI.

Accesos remotos

El departamento de TI puede acceder de forma remota a los equipos de cómputo que tiene a su cargo, con la aceptación previa del custodio, para de esta manera brindar una solución más rápida a cualquier inconveniente.

Comunicaciones electrónicas

Los siguientes puntos se encuentran estrictamente prohibidos:

- El uso inadecuado de los equipos de comunicación, incluyendo el apoyo a las actividades ilegales, y la adquisición o transmisión de material que viole las políticas de GNN7 TV contra el acoso o la protección de la información confidencial o reservada.

- El envío de spam a través del correo electrónico, mensajes de texto, páginas, mensajes instantáneos, correo de voz, u otras formas de comunicación electrónica.

- Forjar, falsificar, ocultar o suprimir una identidad de usuario en cualquier comunicación electrónica para engañar el destinatario sobre el remitente.

- El uso del correo electrónico o direcciones IP's para participar en una conducta que viola las políticas o directrices de GNN7 TV. Debe ejercer el buen juicio para evitar falsificación o exceso de autoridad en la representación de la opinión de GNN7 TV a través de un grupo de noticias, tablón de anuncios, lista de correo electrónico o a través de un correo electrónico corporativo o publicar la dirección IP que representa a GNN7 TV al público.

Publicidad y actualización

Las condiciones de uso expuestas en el presente documento pueden ser actualizadas por GNN7 TV tras aprobación de la junta directiva.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta; corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red de GNN7 TV y que no estén previstas en las políticas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.2.1.9 Política para el uso correcto del correo electrónico

El propósito de la "Política para el uso correcto del correo electrónico" es establecer políticas para el uso correcto de los recursos de correo electrónico otorgados por GNN7 TV a sus empleados.

Privacidad, confidencialidad y consideraciones de registros públicos.

GNN7 TV hará todos los esfuerzos razonables para mantener la integridad y el funcionamiento eficaz del sistema de correo electrónico, pero se aconseja a los usuarios que los sistemas de correo electrónico no deben ser considerados como un medio seguro para la comunicación de información sensible o confidencial. Debido a la naturaleza y la tecnología de la comunicación electrónica, GNN7 TV no podrá asegurar la confidencialidad del uso individual de los recursos de correo electrónico, ni la confidencialidad de los mensajes particulares que pueden ser creados, transmitidos, recibidos o almacenados por el mismo.

Usos permitidos del correo electrónico.

Usuarios autorizados. Los empleados de GNN7 TV son los únicos autorizados por parte del departamento de TI y RRHH para utilizar el correo electrónico empresarial.

Propósito de uso. El uso del correo electrónico debe estar relacionado con actividades laborales de la organización. Cualquier uso incidental y ocasional de recursos de correo electrónico para fines personales está sujeto a las disposiciones de esta política.

Usos prohibidos del correo electrónico

- Se prohíbe el uso personal que crea un costo directo para GNN7 TV.
- Los recursos de correo electrónico de la corporación no se utilizarán para obtener beneficios económicos personales o con fines comerciales, que no están directamente relacionados a los negocios de GNN7 TV.
- Se prohíbe el envío de correos electrónicos de más de 25MB de tamaño, para el cálculo también se debe tomar en cuenta el número de destinatarios, es decir un mail de 25MB enviado a 2 usuarios se considerará como de 50MB. En caso de que por trabajo se requiera enviar más información, se deberá consultar con el departamento de TI métodos alternativos.
- Los usuarios deberán reportar al área de TI cuando reciban correos de más de 25MB, que pueden en ciertos momentos complicar el tráfico de Internet.
- Envío de copias de documentos que violen las leyes de derecho de autor.
- Incluir en las comunicaciones de correo electrónico los trabajos de otros en violación de las leyes de derechos de autor.
- En el caso de que exista algún error en el envío o recepción del correo electrónico, sólo el dueño de la cuenta autorizará al departamento de TI para que efectúe la respectiva revisión del problema.
- El uso del correo electrónico para acosar o intimidar a otros.

- El uso de sistemas de correo electrónico para cualquier propósito restringido o prohibido por las leyes o reglamentos.

- El intento de acceso no autorizado al correo electrónico o intentar violar las medidas de seguridad en cualquier sistema de correo electrónico, o el intento de interceptar las transmisiones de correo electrónico sin la debida autorización.

- "Snooping", es decir, la obtención de acceso a los archivos o correo electrónico de los demás usuarios con el fin de satisfacer la curiosidad ociosa, sin fines comerciales para GNN7 TV.

- "Spoofing", es decir, la suplantación de identidad en una comunicación por correo electrónico.

Disposiciones generales para el acceso y divulgación.

En la medida permitida por la ley, se reserva el derecho de acceder y divulgar el contenido de la información de propiedad de GNN7 TV a empleados y otros usuarios a través de correo electrónico sin el consentimiento de GNN7 TV. A los empleados se les aconseja que los sistemas de correo electrónico deben ser tratados como un sistema de archivos compartido, es decir, con la expectativa de que las comunicaciones enviadas o recibidas por negocios o con el uso de los recursos se pueden hacer disponibles para su revisión por un funcionario autorizado para fines relacionados con las actividades de GNN7 TV. Cualquier usuario de los recursos de correo electrónico, que haga uso de un dispositivo de encriptación para limitar o impedir el acceso a su correo electrónico deberá facilitar el acceso a este tipo de comunicaciones cifradas, cuando así lo solicite la autoridad correspondiente de GNN7 TV.

Vigilancia de las comunicaciones.

GNN7 TV no supervisará el correo electrónico continuamente, pero puede hacerlo en la medida permitida por la ley las veces que considere necesarias con el fin de mantener la integridad y el funcionamiento eficaz de los sistemas de correo electrónico.

Inspección y divulgación de comunicaciones.

GNN7 TV se reserva el derecho de inspeccionar y dar a conocer el contenido del correo electrónico, en los siguientes casos:

- En el curso de una investigación impulsada por la evidencia de mal uso.
- Para evitar la interferencia con la misión y visión de GNN7 TV.
- Según sea necesario para localizar y evitar que la información confidencial y necesaria para la lógica de negocios de GNN7 TV se encuentre almacenada en cualquier otro medio.
- Se inspeccionará y divulgará el contenido de correo electrónico cuando sea necesario para responder a los procesos legales y cumplir con las obligaciones de GNN7 TV.

Restricciones a la divulgación y uso de información

Los contenidos de las comunicaciones de correo electrónico, cuyos fines, pueden ser revelados sin el permiso del usuario. GNN7 TV procurará abstenerse a la divulgación de comunicaciones, sin crear vergüenza al personal, a menos que dicha revelación sea necesaria para un propósito comercial o por obligación legal.

Procedimientos especiales para aprobar el acceso, divulgación o uso del correo electrónico.

Las personas que necesiten acceder a los diferentes buzones de correo electrónico de otros usuarios, para utilizar y/o divulgar la información de dicho acceso, y que además no cuentan con el consentimiento previo y explícito del usuario, deberán obtener la aprobación por adelantado de tal actividad por las respectivas autoridades de GNN7 TV. El gerente de cada área deberá desarrollar una declaración escrita del procedimiento a seguir para solicitar dicha autorización.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la gerencia y/o recursos humanos. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta. Corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad del uso del correo electrónico de GNN7 TV y que no estén previstas en las políticas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.2.1.10 Política del uso aceptable del internet

El propósito de la "Política del uso aceptable del Internet" es establecer políticas para el uso aceptable del Internet que se encuentra a disposición de todo el personal de GNN7 TV. El departamento de TI es el responsable de administrar el control, definiendo diversos tipos de accesos a Internet y en coordinación con los gerentes y/o jefes de cada área determinará el tipo de acceso de cada usuario. Al utilizar la red empresarial para acceder a Internet, los usuarios deberán cumplir con los siguientes puntos:

Usos permitidos

- Compruebe que cualquier información que es accedida a través de Internet es exacta, completa y actual.
- Comprobar la validez de la información encontrada.
- Respetar la protección legal de los datos y software proporcionados por los derechos de autor y licencias.
- Informar de inmediato al departamento de TI de cualquier hecho inusual.

Usos prohibidos

- Queda terminantemente prohibido acceder a páginas web que permitan vulnerar los controles de seguridad (hacking) que conlleven riesgos informáticos de GNN7 TV, así como páginas que sean fuente de virus, malware, spyware, phishing, etc.

- No descargar contenidos de sitios web a menos que se relacionen con el trabajo.

- No descargar textos, imágenes o videos que contienen material de carácter político mal fundamentado, pornográfico, racista, o que incite a la violencia, el odio o cualquier otra actividad ilegal.

- El uso de redes o programas que sirvan para intercambio de cualquier tipo de archivos (par a par) se encuentran totalmente prohibidas y solo pueden ser utilizadas con la aprobación y activación de los permisos por parte del departamento de TI.

- No descargar e instalar software de Internet en los equipos informáticos corporativos.

- Los programas de mensajería instantánea o chat como: Yahoo Messenger, ICQ, Skype o cualquier otro que sirva para el mismo objetivo, son completamente prohibidos tanto su uso como su instalación. En caso de ser requerido deberá ser comunicado al departamento de TI.

- No utilizar las computadoras de la organización para la entrada no autorizada de cualquier otra computadora a la red corporativa utilizando clientes de acceso remoto sobre web.

- Está prohibida la conexión a Internet a través de Wifi de cualquier computador externo, a menos que exista previa aprobación de gerencia, un jefe de área o el jefe del departamento de TI.

- No utilizar el acceso a Internet para transmitir material confidencial, políticos, obsceno, amenazador, o acosador.

Se deberá tener en cuenta lo siguiente:

- Toda la actividad en Internet es monitoreada y registrada.
- Todos los materiales consultados se escanea en busca de virus.
- Todo el contenido visualizado se analiza en busca de material ofensivo.
- Cualquier duda sobre el acceso a Internet consultar con el departamento de TI.
- Cualquier incumplimiento a la "Política del uso aceptable de Internet" puede llevar a una acción disciplinaria.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta; corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red de GNN7 TV y que no estén previstas en las políticas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.2.1.11 Política para la reubicación de los activos de información

El propósito de este documento es establecer políticas para que los equipos informáticos de GNN7 TV sigan un proceso adecuado para su reubicación dentro o fuera de la organización. Los sistemas de tecnología de información están sujetos a procesos formales de control de cambios. Estos procesos proporcionan un método administrativo y ordenado para los cambios solicitados, los cuales deben ser probados, aprobados, registrados y comunicados antes de su implementación dependiendo del tipo de activo.

Las razones por las cuales se requiera el movimiento físico de un activo de información están detalladas a continuación:

- Solicitud de cambio físico basado en la necesidad del usuario.
- Recomendaciones y/o requerimiento de cambios por clientes o proveedores externos.
- Actualización de hardware y/o software.
- Adquisición y/o implementación de nuevo hardware o software.
- Fallos de hardware o software que apliquen garantía de fábrica.
- Cambios o modificaciones en la infraestructura.
- Cambios ambientales (aire acondicionado, remodelación en el centro de cómputo, etc.)
- Acontecimientos imprevistos.
- Mantenimiento periódico.
- Mejoras y modificaciones.

A continuación se destacan los procedimientos de control para reubicación de activos:

- El solicitante deberá presentar el documento impreso del "Formulario de solicitud de reubicación de los activos informáticos" (Anexo #3) al personal del departamento de TI.
- Asignación de un responsable de cambios y control de los mismos.
- Deben existir revisiones previas a cualquier cambio físico de los activos de información para garantizar su viabilidad.
- Notificar a los usuarios cada cambio de ubicación de activos de información.

- La viabilidad de un cambio se determinará mediante una revisión previa a la nueva ubicación del activo, esto incluye la disponibilidad de: puntos eléctricos, punto de red, espacio físico, condiciones ambientales óptimas y muebles de oficina (escritorio).

- Todos los cambios físicos de los equipos de cómputo deberán registrarse a través del "Formulario de registro de reubicación de activos informáticos" (Anexo #4).

- Todos los equipos que sean reubicados deberán ser notificados por escrito al administrador de activos fijos y al departamento de TI para la actualización en el sistema.

- Para la reubicación de un equipo de cómputo se hará únicamente bajo la autorización del responsable departamental.

Roles y cumplimientos generales

- **Departamento de TI:** Su responsabilidad es supervisar, cumplir y hacer cumplir la política de control de cambios y todos los procesos que en ella se detallen.

- **Usuarios finales:** Enviar solicitudes de cambios, participar en las pruebas de usuario, si es necesario cerrar el caso.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad de GNN7 TV que se infrinjan durante el proceso de cambios físicos de activos deberá ser sancionada de acuerdo a los reglamentos internos de GNN7 TV. En caso de que la infracción no esté detallada en los reglamentos internos de GNN7 TV, esta deberá ser analizada por los responsables administrativos de GNN7 TV y serán estos los que decidan la sanción para el infractor.

3.2.1.12 Política para la comunicación inalámbrica

Políticas generales

El propósito de este documento es establecer políticas para la comunicación en las redes inalámbricas de GNN7 TV. Estas normas se aplican a todos los dispositivos de infraestructura inalámbrica que se conectan a la red corporativa o se encuentren al interior de GNN7 TV proporcionando conectividad inalámbrica a dispositivos de punto final, incluyendo ordenadores portátiles, ordenadores de escritorio, teléfonos celulares, tabletas y asistentes digitales personales (PDA). Esto también incluye cualquier forma de dispositivo de comunicación inalámbrica capaz de transmitir paquetes de datos.

Requisitos generales de acceso a la red inalámbrica.

Todos los dispositivos de infraestructura inalámbrica que residan en las instalaciones de GNN7 TV y se conecten a la red empresarial o faciliten el acceso a información clasificada como confidencial, altamente confidencial, o restringida deberán cumplir los siguientes puntos:

- Cumplir con las normas especificadas en los estándares de comunicación inalámbrica.
- Utilizar protocolos de autenticación e infraestructura aprobados por la institución.
- Utilizar protocolos de cifrado aprobados por GNN7 TV.
- Mantener una dirección de hardware (dirección MAC) que se pueda registrar y dar seguimiento.
- No deben interferir con las implementaciones de acceso inalámbrico mantenidos por otros dispositivos.
- Regirse a las políticas de acceso a Internet para las redes inalámbricas establecidas en GNN7 TV.

Requisitos de los dispositivos inalámbricos aislados

Todos los dispositivos de infraestructura inalámbrica que permiten conexión deben cumplir esta política tomando en cuenta los siguientes aspectos:

- La red administrativa debe ser distinta a la red inalámbrica para así evitar accesos no autorizados a los sistemas transaccionales de la organización.
- Los dispositivos conectados a la red inalámbrica no deben interferir con las implementaciones de acceso inalámbrico mantenidos por otros dispositivos.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad detalladas en este documento deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta. Corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red inalámbrica y que no estén dentro de las políticas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.2.1.13 Política de conciencia y formación para la seguridad de la información

Política general

Periódicamente se deberá ejecutar un plan de acción, formación y concienciación al personal acerca de las políticas de seguridad de la información, procedimientos, sanciones y responsabilidades que dictaminen las mismas. Dentro de la formación se debe incluir a los empleados nuevos de GNN7 TV o en su defecto al personal contratado con anterioridad que deberá asistir y/o tomar el curso de actualización periódica acerca de la concienciación sobre la seguridad.

Los puntos a tratar en la capacitación son los siguientes:

- Mejorar la conciencia a los usuarios acerca de la necesidad de proteger los recursos de información.
- Asegurar que los usuarios entiendan claramente sus responsabilidades para proteger los recursos informáticos y de información tangibles o no.
- Asegurar que los usuarios se encuentren bien informados acerca de las políticas de GNN7 TV y las prácticas de seguridad de la información.
- Desarrollar habilidades y conocimientos para que los usuarios puedan realizar su trabajo con seguridad.

Personal en entrenamiento

Algunos usuarios de la red pueden requerir una formación más avanzada o especializada que la capacitación general de concienciación impartida, con el fin de apoyar a los niveles de seguridad de GNN7 TV. Por ejemplo, los gerentes, administradores de sistemas y administradores de datos pueden requerir comprender las consecuencias de seguridad, factores de costos y requisitos de seguridad para productos específicos. La educación especializada para el personal del departamento de TI en materia de seguridad se proporcionará según sea necesario mediante cursos formales externos y programas de certificación.

Cumplimiento y ejecución

La política se aplica a todos los usuarios incluyendo a trabajadores temporales y demás usuarios autorizados. Las personas que violen las normas de seguridad indicadas durante el entrenamiento estarán sujetas a una serie de sanciones (determinadas y ejecutadas por GNN7 TV), incluyendo acciones disciplinaria. El departamento de TI tendrá bajo su responsabilidad informar todas las violaciones a las autoridades respectivas.

Acción disciplinaria

Cualquier violación a las políticas de conciencia y formación de la seguridad de la información deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta. Corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa el cumplimiento y seguimiento de las normas establecidas en este documento y que no estén previstas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.3 Dominio - Seguridad física y del entorno

3.3.1 Objetivo de Control - Seguridad de los equipos

OBJETIVO: Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización. Se debiera proteger el equipo de amenazas físicas y ambientales. La protección del equipo (incluyendo aquel utilizado fuera del local y la eliminación de propiedad) es necesaria para reducir el riesgo de acceso no autorizado a la información y proteger contra pérdida o daño, esto también debiera considerar la ubicación y eliminación del equipo. Se pueden requerir controles especiales para proteger el equipo contra amenazas físicas, y salvaguardar los medios de soporte como el suministro eléctrico y la infraestructura del cableado.

3.3.1.1 Auditoria - Servicios de soporte

Objetivo

El objetivo de este control es que GNN7 TV cuente con mecanismos definidos que brinden apoyo y soporte sobre los sistemas de información permitiendo así proteger a todos los activos informáticos contra fallas de energía y fluctuaciones en los suministros eléctricos.

Alcance

Se tiene como alcance establecer mecanismos de prevención sobre incidentes eléctricos y así asegurar que la energía fluya de forma continua y que los activos informáticos no se vean afectados y puedan solventar de forma eficiente las interrupciones eléctricas.

Auditoria

GNN7 TV tiene varios mecanismos de apoyo continuo de energía entre ellos cuenta con un SAI (Sistema de Alimentación Ininterrumpida) centralizado que protege a los equipos ante fluctuaciones eléctricas y de generadores de corriente que se activan en el caso de un apagón prolongado.

Los SAI y generadores dan servicio al edificio a través de tomas eléctricas aterrizadas distribuidas de forma equitativa en algunas áreas. Actualmente los mantenimientos e instalaciones eléctricas son gestionados por el personal especializado de GNN7 TV que no es parte del departamento de TI, a los cuales también se les reporta los fallos energéticos para que tomen las precauciones debidas ante dicha problemática.

Recomendaciones

Aunque el dispositivo SAI existente cumple con el requerimiento de brindar servicio eléctrico luego de una interrupción, se recomienda a los encargados siempre buscar alternativas para brindar un mejor soporte eléctrico, puesto que por el tipo de negocio se requiere que los activos informáticos funcionen de manera ininterrumpida. Se recomienda también al área responsable que realicen mantenimientos preventivos con mayor frecuencia y a su vez pruebas periódicas para verificar que la protección se encuentra siempre activa, todo esto debe ser en coordinación con los demás departamentos, para evitar cualquier tipo de inconvenientes.

3.3.1.2 Auditoria - Mantenimiento de los equipos de computación

Objetivo

El objetivo de este control es que el departamento de TI tenga planes de mantenimiento preventivo y correctivo para los activos informáticos y de esta forma de esta manera preservar en óptimas condiciones su rendimiento y operatividad.

Alcance

El alcance de este control es que todos los activos informáticos y de información de GNN7 TV formen parte de un plan de mantenimiento preventivo y correctivo a nivel físico y lógico.

Auditoria

GNN7 TV actualmente no cuenta con los siguientes controles:

- Planificación periódica de mantenimiento físico y lógico para los activos computacionales.
- El departamento de TI ejecuta mantenimientos reactivos y no proactivos de los activos informáticos y de la información.
- No existe un historial de los mantenimientos realizados sobre los activos informáticos de GNN7 TV.
- No existe una base de conocimientos documentada previa al mantenimiento lógico o físico sobre los activos informáticos de GNN7 TV.

Recomendaciones

Se recomienda al departamento de TI implementar los siguientes puntos:

- Cada mantenimiento de los activos informáticos deberá ejecutarse siguiendo la guía "Procedimiento para mantenimiento de activos informáticos" (Ver 3.3.1.3).

- El único personal autorizado para brindar servicio técnico, efectuar reparaciones y dar mantenimiento físico y lógico a los equipos de computación son los miembros del departamento de TI.

- En caso de solicitar servicio de mantenimiento a un proveedor y/o fabricante, se deberá pedir autorización al jefe del área de TI.

- Registrar todas las reparaciones o eventos concernientes al mantenimiento preventivo y correctivo de todos los equipos de computación.

- En caso de que el mantenimiento de un activo informático sea realizado por el departamento de TI e incluso por terceros, fuera de las instalaciones de GNN7 TV, se deberá seguir sin excepción las recomendaciones dadas en el control 3.3.1.4 de esta auditoría.

- Crear base de conocimientos en la que se registren métodos y herramientas utilizadas en mantenimientos físicos y lógicos a los activos informáticos y de información realizados anteriormente.

- Si los activos informáticos de GNN7 TV cuentan con una póliza de seguro, cumplir con los requerimientos impuestos por la compañía aseguradora.

3.3.1.3 Política para el mantenimiento de activos informáticos

El personal responsable de gestionar el mantenimiento de los activos deberá seguir las recomendaciones definidas a continuación:

- Establecer un cronograma de mantenimientos preventivos y correctivos que involucre a todos los dispositivos de computación de las distintas áreas de la institución.

- Deberá registrar los mantenimientos preventivos y correctivos de los equipos de computación de la organización a través del "Formulario de registro de mantenimiento de activos informáticos" (Anexo #6).

- Mantener en concordancia las especificaciones técnicas y periodos de mantenimiento recomendados por algún proveedor y/o fabricante para ciertos activos informáticos y de la información.

- El mantenimiento de los activos informáticos, la conservación de su instalación, la verificación de su seguridad física, y el acondicionamiento específico para cada usuario GNN7 TV le corresponde al personal del departamento de TI.

- En caso de ser requerido el servicio de un tercero este debe tener previa autorización del jefe del área de TI.

- Los mantenimientos de los dispositivos de computación deberán solicitarse al departamento de TI a través del "Formulario de solicitud de mantenimiento de activos informáticos" (Anexo #5).

- Toda petición de mantenimiento deberá contener sin excepción las firmas de autorización del el custodio, el jefe de área y el jefe del área de TI.

- Cuando un ordenador requiere mantenimiento, ambas partes (El departamento de TI y el custodio) deberá coordinar la fecha en que se va a efectuar dicho mantenimiento.

- Una vez programado el mantenimiento de un activo informático, este debe ser comunicado personalmente y vía correo electrónico a todas las partes involucradas, este debe contener todos los detalles del mismo, incluida la fecha y hora.

- Queda estrictamente prohibido dar mantenimiento a computadoras, que no sean propiedad de GNN7 TV, salvo con el visto bueno de una autoridad, gerencia técnica y jefe de TI.

3.3.1.4 Auditoria - Seguridad de equipos de computación fuera de la empresa.

Objetivo

El objetivo de este control es implementar políticas de seguridad para los activos informáticos y de información que se encuentren fuera de las instalaciones de GNN7 TV por motivos de reparación, garantía o calidad de préstamo, tomando en cuenta todos los riesgos de seguridad que esto implica y evitar posibles casos de estafa, pérdidas o robo de información.

Alcance

El alcance de este control proteger todos los activos informáticos y sobre todo la información que estos contienen cuando se encuentran fuera de las instalaciones de GNN7 TV; los dispositivos que deben cumplir con esta política son todos aquellos que procesan o almacenan información confidencial y de propiedad de GNN7 TV, por ejemplo:

- Computadores de escritorio y portátiles.
- Dispositivos móviles como celulares y tabletas.
- Dispositivos de almacenamiento extraíble (memorias USB, memorias SD, discos duros externos, CDs, DVDs, etc.).

Auditoría

GNN7 TV no cuenta con mecanismos definidos para la correcta manipulación de los activos informáticos fuera de la institución, ni para el personal responsable en autorizar la salida del equipo, por lo que los usuarios actualmente pueden portar o movilizar los diferentes dispositivos o equipos de cómputo de propiedad de GNN7 TV en sitios que conllevan riesgos altos como pérdida y robo del activo, y sobre todo robo de la información.

Recomendaciones

Se recomienda tomar en cuenta los siguientes puntos para todos los activos informáticos que almacenen y procesen información que deban trasladarse fuera de las instalaciones de la empresa:

- Todos los activos informáticos y de información antes de salir de GNN7 TV deben cumplir con las normas establecidas en la "Política de seguridad de los equipos de computación fuera de GNN7 TV". (Ver 3.3.1.5).
- El personal del departamento de TI deberá controlar la salida de los dispositivos de computación a través del "Acta de registro de salida de equipos de la organización". (Ver 3.3.1.6).
- Los equipos de computación que salgan de las instalaciones de GNN7 TV deben hacerlo bajo la autorización del jefe inmediato del departamento de TI y el área de activos fijos de la organización.
- El departamento de TI debe implementar controles para el trabajo fuera de GNN7 TV, estos incluyen archivos protegidos por contraseñas, controles de acceso para las computadoras, etc.
- El área de TI debe verificar que las aplicaciones y el sistema operativo del activo cuente con las actualizaciones de seguridad necesarias, entre ellas los parches del sistema operativo, base de datos y antivirus actualizado, etc.

3.3.1.5 Política de seguridad de los equipos de computación fuera de GNN7 TV

El personal que requieran trasladar dispositivos informáticos fuera de las instalaciones de GNN7 TV deberá seguir las recomendaciones definidas a continuación:

- Todos los activos informáticos deben contar con un seguro adecuado para proteger el equipo contra robo o daños.

- Solicitar autorización al personal del departamento de TI a través del "Formulario de solicitud de salida de equipos de computación de la institución" (Ver anexo #7).
- Toda autorización deberá ser firmada por el solicitante, el jefe de área, el jefe del área de TI y el jefe del área de activo fijo.
- Se deben considerar las instrucciones de los fabricantes para proteger el equipo durante el transporte.
- Todos los activos informáticos al estar fuera de GNN7 TV, siempre deben estar en posesión del custodio, nunca debe ser manipulado por un tercero.
- Si por motivos de viaje una persona solicita llevar uno o más de los activos informáticos bajo su custodia, este debe asumir toda la responsabilidad de lo que pueda ocurrir con el mismo.
- Cuando un activo informático deba ser movilizado por motivos de viaje de su custodio, durante el viaje el equipo debe siempre ser llevado como equipaje de mano y de ser posible, oculto.

3.3.1.6 Acta de registro de salida de equipos de la organización

Utilizando este formato se podrá llevar un registro de salidas de los activos informáticos de GNN7 TV.

Acta de Registro de Salida de Equipos de la Organización										
Fecha de Salida	Nombre del Solicitante	Departamento	Jefe de Área	Motivo de Salida del Equipo	Código de Inventario	Equipo	Marca	Modelo	Número de Serie	Detalles de sus partes

Figura #3.47: Acta de registro de salida de equipos de la organización

Elaborado por: Autores

3.3.1.7 Auditoria - Reutilización y retirada segura de equipos de computación

Objetivo

El objetivo de este control es gestionar la baja y el destino final de los dispositivos informáticos de la organización que por su estado físico o cualidades técnicas no resulten útiles para el servicio a que se encuentran destinados.

Alcance

El alcance de este control es aplicable en todas las áreas de la organización las cuales hagan de uso general de algún bien informático que necesite ser reemplazado por encontrarse en mal estado físico o lógico.

Auditoría

GNN7 TV no cuenta con procedimientos que permitan ejecutar y controlar de forma correcta la reutilización y retirada segura de los activos informáticos, lo cual impide que el departamento de TI obtenga reportes acerca del estado de los equipos ni tampoco el poder gestionar el destino final de los dispositivos dados de baja.

Recomendaciones

Se recomienda tomar en cuenta los siguientes puntos para todos los activos computacionales dados de baja en la organización:

- El personal del departamento de TI deberá cumplir con las normas establecidas en la "Política de reutilización y retirada segura de los equipos de computación". (Ver 3.3.1.8).
- El departamento de TI deberá efectuar pruebas y análisis de los activos de computación que presenten fallas o características obsoletas para comprobar

que tales equipos no pueden ser reubicados dentro de la organización y que no son de utilidad para la misma.

- La gerencia administrativa y gerencia financiera junto con el área de activos fijos serán los responsables de revisar los reportes enviados por el área de TI quien tendrá a su cargo el dictamen final, debiendo informar la resolución al departamento de sistemas para gestionar el destino final de los activos informáticos.

3.3.1.8 Política de reutilización y retirada segura de los equipos de computación

El personal responsable de la reutilización y retirada segura de los dispositivos informáticos deberá seguir las recomendaciones definidas a continuación sin excepción:

- Registrar las pruebas y análisis de los activos de computación que presenten fallas o características obsoletas a través del "Formulario de registro de los activos fijo computacionales dados de baja" (Anexo #8).
- Reportar periódicamente los activos de computación que por su estado físico o cualidades técnicas no prestan actualmente el servicio para lo cual fueron adquiridos.
- Dictaminar el estado del activo informático, así como sus posibilidades de reutilización o la reutilización de algunas de sus partes, las cuales deben encontrarse funcionales.
- Los equipos y accesorios de computación que no sean útiles se ubicarán en un lugar físico específico que determine el departamento de TI y la gerencia administrativa.
- El departamento de TI y las entidades como la gerencia administrativa y financiera en conjunto con el área de activos fijos decidirán qué hacer con cada activo dado de baja.

3.4 Dominio - Gestión de operaciones y comunicaciones

3.4.1 Objetivo de Control - Responsabilidades y procedimientos de operación

OBJETIVO: Asegurar la operación correcta y segura de los medios de procesamiento de la información. Se debieran establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados. Cuando sea apropiado, se debiera implementar la segregación de tareas para reducir el riesgo de negligencia o mal uso deliberado del sistema.

3.4.1.1 Auditoria - Documentar procedimientos de operación

Objetivo

El objetivo de este control es que el departamento de TI cuente con manuales de operación para todas las herramientas que administran el SGSI y que todo procedimiento de control sea debidamente documentado para mantener la infraestructura tecnológica bajo las políticas vigentes.

Alcance

El alcance de este control es que el departamento de TI cree un repositorio con todos los manuales de operación necesarios para administrar el SGSI, esto incluye manuales para todas las aplicaciones (software) y procedimientos documentados que estén en concordancia con las políticas de seguridad vigentes.

Auditoria

El resultado de la auditoría a este control arroja lo siguiente:

- El departamento de TI no cuenta con manuales para todas las herramientas que administran el SGSI, como por ejemplo antivirus, correos, proxy, etc.

- El departamento de TI no cuenta con manuales de operación para todos los procedimientos internos vigentes.

Recomendaciones

Para los manuales de operación de las herramientas que administran el SGSI:

- Se recomienda tener un manual para cada herramienta informática, este debe contener información actualizada sobre el uso y configuración de las diferentes versiones de dichas herramientas.

Para los procedimientos del departamento:

- Debe existir registros de todas las actividades en el SGSI asociadas con los medios de procesamiento de la información y comunicación, se recomienda tomar en cuenta todos los procedimientos propuestos en este proyecto.
- Para la ejecución de cada tarea se debe especificar por escrito detalles como: horarios/tiempos de ejecución, instrucciones para el manejo de errores u otras condiciones excepcionales, contactos de soporte, instrucciones para el manejo de herramientas especiales en caso de ser necesarias, procedimientos de reinicio y recuperación del sistema por fallas.
- Los procedimientos de operación y los procedimientos documentados para las actividades del sistema deben ser tratados como documentos formales y deben tener la aprobación de la jefatura TI y gerencia técnica.

3.4.1.2 Política para documentar procedimientos de operación

La “Política para documentar procedimientos de operación” abarca los manuales de herramientas provistos por fabricantes, recomendaciones de proveedores y procedimientos de control y operación del departamento de TI.

Todos los manuales y procedimientos utilizados por el departamento de TI deben ser tratados como documentos formales y deben tener la aprobación de la jefatura de TI y gerencia técnica.

Para las herramientas usadas por el departamento de TI se deben tener presente lo siguiente:

- En caso de no poseer uno o más manuales de las herramientas informáticas, estos deben ser descargados de los sitios oficiales de cada fabricante.
- El departamento de TI debe tener un manual para cada herramienta informática ya sea de servidores, estaciones de trabajo, aplicaciones del usuario, herramientas de control usadas por el departamento de TI, etc.
- Todos los manuales deben contener información actualizada, hacer revisiones periódicas a los sitios oficiales del fabricante para estar al tanto de novedades como: parches de seguridad, nuevas versiones de la herramienta, consejos para el buen uso, guías de usuarios actualizadas, etc.
- En caso de que uno o más fabricantes no dispongan del manual de operación para sus herramientas, este debe ser creado por el departamento de TI consultando sitios de confianza y haciendo pruebas de funcionamiento.

Para los procedimientos de operación y control del departamento de TI se deben tomar en cuenta los siguientes puntos:

- El departamento de TI debe tener un manual para cada procedimiento de operación y control implementado en el SGSI.
- El departamento de TI debe documentar todas las actividades en el SGSI asociadas con los medios de procesamiento de la información y comunicación.

- Todo manual será revisado periódicamente y modificado en caso de haber nuevas implementaciones o que los procesos de operación hayan cambiodo.
- En caso de que el departamento de TI no disponga de un manual de operación este debe ser creado con información detallada para evitar confusiones, evitar operaciones incorrectas o diferencias de criterios dentro del departamento.
- Para la ejecución de cada tarea se debe especificar por escrito detalles como: horarios/tiempos de ejecución, instrucciones para el manejo de errores u otras condiciones excepcionales, contactos de soporte, instrucciones para el manejo de herramientas especiales en caso de ser necesarias, procedimientos de reinicio y recuperación del sistema en caso de falla.

3.4.1.3 Auditoria - Gestión de cambios.

Objetivo

El objetivo principal del control de la gestión de cambios es asegurar que se utilizan procedimientos y métodos estandarizados para el manejo eficiente y puntual de todos los cambios aprobados, a fin de minimizar su impacto en la calidad de los servicios y la continuidad del negocio.

Alcance

El alcance de este control es supervisar la gestión para todos los cambios a nivel de los servicios informáticos que vayan a realizarse en cualquier elemento de configuración que forme parte del SGSI de GNN7 TV.

Auditoria

El área de TI no cuenta con procesos definidos para la gestión y registro sobre cambios realizados a sus servicios informáticos, provocando así que exista falta de conocimiento general sobre actualizaciones, migraciones, movimientos y configuraciones realizadas por los miembros del área.

Recomendaciones

Para una correcta gestión de cambios se recomienda tomar en cuenta lo siguiente:

- Todos los cambios realizados, su gestión y procesos, deben cumplir en su totalidad con lo expuesto en la "Política de gestión de cambios" (Ver 3.4.1.4).
- Antes de implementar un cambio, este debe ser revisado y aprobado por los responsables administrativos del mismo en conjunto con el jefe del departamento de TI y el gerente técnico en caso de ser necesario.
- Registrar todos los cambios, asignando un responsable, prioridad, categoría, y demás aspectos para una correcta gestión.

Diagrama de proceso para la gestión de cambios (recomendado)

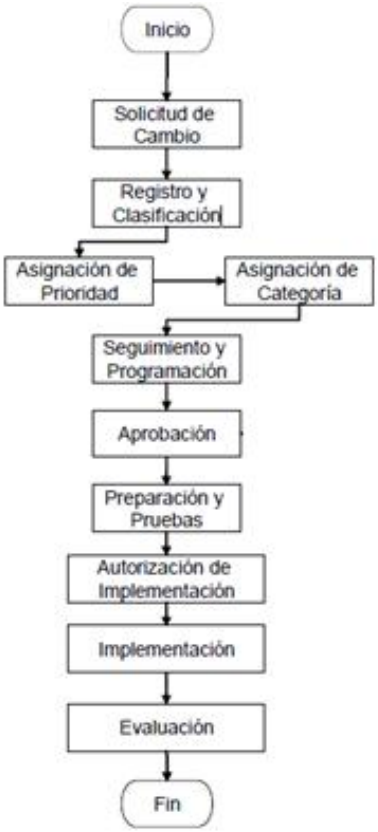


Figura #3.48: Diagrama de proceso para la gestión de cambios (recomendado)

Elaborado por: Autores

3.4.1.4 Política para la gestión de cambios

La "Política para la gestión de cambios" define los mecanismos para tramitar el visto bueno de los cambios propuestos para la infraestructura informática y sus procesos.

- Las únicas personas que pueden dar dicha autorización son: el jefe del área de TI y el gerente técnico.
- El jefe del departamento de TI es el responsable de dirigir y controlar que los cambios efectuados por el personal operativo del área sean implementados de forma eficiente, efectiva, con mínimo riesgo y que el funcionamiento de los sistemas no se afecten provocando problemas en la continuidad del negocio.
- Los miembros del departamento de TI son responsables de la administración de los procesos de cambio que pueden ser desde equipos de comunicación, software, cambios de hardware, documentación y procedimientos asociados a la ejecución, soporte y mantenimiento de sistemas en producción.

Procedimientos para la gestión de cambios

Solicitud, planificación e implementación del cambio

- Recibir la solicitud de cambio generada por cualquier usuario del servicio.
- Clasificar la solicitud de cambio de acuerdo a su prioridad y categoría.
- Programar el cambio y definir un plan de control del cambio.
- Decidir si el cambio se autoriza o no.
- Hacer una preparación para la ejecución y en caso de requerirse realizar las pruebas respectivas antes de ejecutar el cambio.
- Programar el despliegue de cambios luego de pruebas exitosas realizadas.
- Implementar el cambio de acuerdo a la programación y plan de cambio.
- Evaluar el cambio después de su implementación total.
- Cerrar el ciclo del cambio.

En caso de ser requerido por el departamento de TI, se debe adjuntar al formato de solicitud de cambios y toda la documentación que soporte la planeación del cambio.

Todos los cambios deben ser ejecutados como parte del desarrollo de un plan adecuado, el cual debe registrar sus resultados y pruebas conforme a su diseño y las necesidades de GNN7 TV. Estos resultados deben ser guardados como memorias del cambio.

Informes de gestión

- Definir los indicadores que tengan significado específico en los cambios que permitan identificar tendencias, condiciones de alerta, impacto del cambio, velocidad y efectividad del cambio.
- Medir los indicadores definidos en cada uno de los cambios ejecutados.
- Realizar el reporte de los cambios relevantes para los directivos de GNN7 TV, y para los encargados de monitorear los cambios realizados.

3.4.1.5 Auditoria - Segregación de tareas

Objetivo

El objetivo de este control es que cada uno de los miembros del departamento de TI tenga asignadas responsabilidades y tareas específicas para así cubrir todas las necesidades de la infraestructura tecnológica de GNN7 TV.

Alcance

El alcance de este control es que las tareas de administración del SGSI de GNN7 TV tengan un responsable, para así evitar riesgos de mal manejo no intencional y evitar modificaciones no autorizadas a los activos informáticos o configuraciones de los recursos de red.

Auditoria

Luego de realizar entrevistas a los miembros del departamento de TI y al jefe del departamento se pudo extraer lo siguiente:

- El departamento de TI actualmente cuenta con 6 miembros cuyos cargos son: Jefe de tecnologías de la información, Coordinador de infraestructura y redes, Coordinador de sistemas multimedia, Coordinador de seguridad informática y helpdesk, y dos asistentes de sistemas.
- A pesar de tener cargos diferentes, en la práctica varias tareas se comparten e incluso no van acordes al cargo que poseen.

Recomendaciones

GNN7 TV al no cumplir totalmente con este control, se recomienda lo siguiente:

- Segregar debidamente las tareas y responsabilidades en el SGSI de GNN7 TV.
- En la medida que el número de miembros del departamento de TI varíe, mantener este principio mientras sea posible y practicable.
- Las auditorías a realizarse deben manejarlas de forma independiente para cada miembro del departamento de TI.

3.4.2 Objetivo de Control - Protección contra el código malicioso

OBJETIVO: Proteger la integridad del software y la integración. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados. El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como virus de cómputo, virus de red, caballos troyanos y bombas lógicas. Los usuarios debieran estar al tanto de los peligros de los códigos maliciosos.

3.4.2.1 Auditoria - Controles contra el código malicioso

Objetivo

El objetivo de este control es proteger la integridad del software y la información de GNN7 TV tomando las debidas precauciones para evitar y detectar la introducción de código malicioso y códigos no-autorizados.

Alcance

El alcance de este control es definir políticas que ayuden a proteger la integridad del software y los medios de procesamiento de la información, para así reducir el riesgo de introducción de código malicioso a los activos de información de GNN7 TV. Además, establecer un plan de capacitación para que los usuarios estén al tanto de los peligros que implica introducir malware y así puedan tener precauciones mínimas para salvaguardar la información de los equipos de los cuales son responsables.

Auditoria

De la auditoría realizada a los controles anti-malware podemos extraer lo siguiente:

- El departamento de TI no realiza revisiones periódicas generales a la consola de administración del antivirus (tareas programadas, configuraciones, etc.).
- No existen revisiones periódicas del antivirus instalado en cada computador.
- Existe la tarea programada en la consola de administración para la descarga periódica de actualizaciones de la base de datos de virus pero no se realizan revisiones para comprobar que la base fue actualizada y las políticas de actualización fueron debidamente propagadas a los clientes.
- GNN7 TV cuenta con una herramienta para el control de dispositivos extraíbles en el cual se configuran perfiles de bloqueos/permisos de lectura/escritura según la necesidad del usuario sobre los medios extraíbles, pero actualmente la herramienta no está totalmente operativa.

- La navegación por Internet no está protegida, existen bloqueos de páginas web por contenido, pero no cuentan con una herramienta que busque malware en los paquetes entrantes.
- El servicio de correos se encuentra protegido con una herramienta de búsqueda de malware.

Recomendaciones

La protección contra código malicioso se debe basar en la detección y reparación de software, conciencia de seguridad, y los apropiados controles de acceso al sistema y gestión del cambio. Se recomienda considerar los siguientes puntos:

- Establecer una política donde se prohíba el uso de software no autorizado.
- Establecer una política formal para proteger a GNN7 TV contra riesgos asociados con la obtención de archivos a través de redes externas o cualquier otro medio, indicando las medidas de protección a tomarse.
- Programar jornadas de capacitación para los usuarios sobre riesgos y usos de herramientas para detección de código malicioso.
- Preparar planes apropiados para la continuidad del negocio para recuperarse de ataques de códigos maliciosos, incluyendo restablecer equipos y datos.
- Implementar procedimiento para la recolección regular de información, como suscribirse a listas de correos y/o chequear páginas web que dan información sobre códigos maliciosos nuevos.
- Implementar procedimientos para verificar la información relacionada con el código malicioso y para asegurar que los boletines de advertencia sean exactos e informativos.
- Instalar y actualizar regularmente el software para la detección o reparación de código malicioso en las computadoras y medios como un control preventivo o una medida rutinaria; los chequeos llevados a cabo debieran incluir:

- Revisar archivos en medios electrónicos, medios ópticos y los archivos recibidos a través de la red para detectar código malicioso antes de utilizarlo.
- Analizar los adjuntos y descargas desde correos para detectar códigos maliciosos antes de utilizarlos, esto debe llevarse a cabo en lugares diferentes; por ejemplo, servidores de correo electrónico y computadoras.
- Analizar las páginas web para detectar códigos maliciosos.

3.4.2.2 Gestión para el control de malware

Este procedimiento es el que deben seguir todos los miembros de GNN7 TV para evitar la introducción de código malicioso y así contribuir a la protección de los datos y los sistemas informáticos y de la información de la organización.

Responsabilidades

Jefe del departamento de TI / Coordinadores de infraestructura y seguridad informática.

- Definir las políticas generales para el control de malware.
- Definir los procedimientos para el control de malware.
- Establecer reglas para el software antivirus, firewall, sistema perimetral, etc.
- Coordinar la implementación de herramientas para el control de malware en las estaciones de trabajo en conjunto con todo el personal TI.
- Monitorear periódicamente que el servicio de antivirus, sistema perimetral y firewall estén funcionando con normalidad.
- Revisar periódicamente las estadísticas del sistema antivirus de las estaciones de trabajo, servidores y todos los medios de procesamiento de información.
- La difusión de las políticas generales a todos los jefes departamentales, responsables y custodios de los activos de información.

Coordinador de helpdesk / Asistentes de sistemas

- Instalar software antivirus en cada estación de trabajo de GNN7 TV.
- Controlar que las estaciones de los usuarios tengan el software antivirus debidamente configurado y actualizado con las últimas definiciones de virus.
- Capacitar al usuario sobre el funcionamiento del software antivirus de su computador, riesgos y acciones a tomar en caso de detectar código malicioso.
- Gestionar periódicamente los respaldos de información de los usuarios para evitar pérdidas de información para el caso de que el activo de computación se encuentre infectado y sea imposible la desinfección provocando con esto la reinstalación y formateo del equipo.

Usuarios

- En caso de alguna infección tomar las medidas necesarias y comunicarse con el departamento de TI inmediatamente para reportar el incidente.

3.4.2.3 Política para el control de malware

Esta política tiene como objetivo establecer los requisitos que deben ser cumplidos por todos los ordenadores conectados a la red de GNN7 TV para asegurar la detección y prevención de virus. La "Política de control de malware" aplica a todos los medios de procesamiento y almacenamiento de información propiedad de GNN7 TV y externos a la organización, esto incluye pero no limita a computadoras de escritorio, computadores portátiles, archivos, servidores, dispositivos móviles, dispositivos de almacenamiento extraíble y cualquier otro recurso tecnológico.

Lineamientos

- Todos los computadores de GNN7 TV deben tener un software de protección contra malware que debe ejecutarse en modo de autoprotección.

- Todas las políticas de control de malware serán puestas en efecto y replicadas mediante reglas administradas con la plataforma de control de malware.
- La definición de las políticas generales están a cargo del jefe del departamento de TI, quien pondrá en conocimiento de las mismas a todo el personal de TI y a los jefes de cada departamento.
- La difusión de las políticas generales a los responsables de cada activo informático está a cargo de todos los miembros del departamento de TI.
- Preparar planes apropiados para la continuidad del negocio luego de recibir algún ataque de código malicioso, incluyendo restablecer equipos y datos.
- El antivirus y la base de datos de virus deben actualizarse periódicamente.
- Si un medio de almacenamiento, dispositivo fijo o móvil está infectado por virus debe ser retirado de la red hasta que sea desinfectado y se encuentre libre de virus.
- El departamento de TI es el responsable de verificar en intervalos de tiempo que las computadoras o medios de almacenamiento estén libres de virus.
- Las actividades con la intención de crear y/o distribuir programas maliciosos en la red interna de GNN7 TV (por ejemplo, virus, gusanos, troyanos, bombas de correo electrónico, etc.) están prohibidas.
- Todos los archivos en medios electrónicos u ópticos, y los archivos recibidos a través de la red deben ser analizados con la herramienta de control de malware para así detectar código malicioso antes de utilizarlo.
- Por ser el Internet una de las principales fuentes de infección de virus, GNN7 TV cuenta con un sistema de protección de malware que analiza y/o desinfecta automáticamente toda información externa proveniente ya sea del correo electrónico o de sitios web maliciosos.
- El control del sistema perimetral de Internet está a cargo del coordinador de infraestructura y redes, y el coordinador de seguridad informática y helpdesk.

- Programar jornadas de capacitación para los usuarios sobre riesgos y usos de herramientas con las que cuentan para la detección de código malicioso.
- Los dispositivos con sistema operativo distinto a los distribuidos por Microsoft utilizan aplicaciones diferentes para el control de malware, pero las políticas generales también se aplican en ellos.

Acción disciplinaria

Cualquier violación a la "Política para el control de malware" y a cualquier norma de seguridad será sancionada de acuerdo a los reglamentos internos de GNN7 TV. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta. Corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red y que no estén previstas en las políticas, serán revisadas por la gerencia para dictar una resolución sujetándose al estado de derecho.

3.4.3 Objetivo de Control - Copias de seguridad

OBJETIVO: Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información. Se debieran establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia para tomar copias de respaldo de los datos y practicar su restauración oportuna.

3.4.3.1 Auditoria - Copias de seguridad de la información

Objetivo

El objetivo de este control es implementar en la organización planes de contingencia y respaldo de información para garantizar la continuidad del negocio y la integridad de la información de vital importancia para GNN7 TV.

Alcance

El alcance de este control es mejorar los planes actuales de contingencia y respaldos de información que posee el área de TI, y que a su vez estos incluyan a todos los equipos administrados por el área, así como también cualquier dispositivo que contenga información de GNN7 TV.

Auditoria

El área de TI lleva a cabo tareas no periódicas para sacar copias o imágenes de los servidores principales y secundarios, las copias obtenidas son almacenadas en algún medio extraíble no seguro, hasta que el personal del departamento de TI se haga responsable y los almacene en una unidad de grabación óptica como un DVD.

GNN7 TV no cuenta con un repositorio general, físico o lógico de las imágenes de los servidores ni tampoco un cronograma que establezca de forma organizada las fechas de respaldo de los equipos críticos para el GNN7 TV.

Actualmente se tienen implementadas soluciones proactivas y reactivas independientes pero que no obedecen a un proceso formal. El departamento de TI cuenta también con servidores virtualizados a los cuales se les saca una copia instantánea de volumen “Snapshot”. Dicha copia tampoco es almacenada en DVDs o algún repositorio general de imágenes que se encuentra organizado bajo un esquema de fechas o nombre de servidor.

Las estaciones de trabajo de GNN7 TV cuentan con un sistema de respaldo de datos llamado “Tivoli Fastback” de IBM; dicho sistema no posee administración ni despliegue de políticas de respaldo de información centralizada, lo cual impide monitorear el estatus de los respaldos realizados en todos los ordenadores de GNN7 TV.

Recomendaciones

Se recomienda elaborar un plan de contingencia y buscar la arquitectura idónea de hardware y software para manejar de forma óptima la gestión de respaldo de información de cada estación de trabajo. Para la correcta elaboración del plan de contingencia de información se deberá seguir los siguientes pasos:

Identificar y priorizar los procesos y recursos vitales.

Se deberá identificar todos los puntos críticos dentro de GNN7 TV. El departamento de TI será el responsable de elaborar un óptimo plan de contingencia y de respaldos de información, deberá ser capaz de establecer prioridades entre los procesos en conjunto con los jefes de cada área.

Análisis de riesgo e impacto.

Analizar el riesgo y el impacto que provocaría algún tipo de desastre u otra interrupción que haga que los recursos críticos de información no se encuentren operativos durante un tiempo, los cuales deberán clasificarse como:

- Desastres naturales (Ej. terremoto, incendios o inundaciones).
- Desastres por falta de servicio (Ej. falta de energía, fallas en la red).
- Ataques a la infraestructura de red (Ej. ataque de denegación de servicio, borrado de información, infección de virus).

Para que el plan de contingencia sea efectivo el departamento de TI deberá tener en cuenta todos los tipos de situaciones que puedan ocurrir dentro de las instalaciones o en las operaciones del negocio. En esta fase intervendrán de manera conjunta el personal de TI, gerencia general y los usuarios finales.

Recomendaciones de protección.

En un buen plan de contingencia deberán establecer políticas de almacenamiento de datos y copias de seguridad de servidores principales y secundarios de cara a una posible recuperación ya sea ante un desastre o ante cualquier despiste por parte de usuarios. Entre las recomendaciones para proteger la información y el estado actual de los servidores se deberá hacer un plan de respaldo de la información (backup) y establecer políticas de copias de seguridad para poder recuperar los datos después de inconvenientes provenientes de fallos en algún servidor y así poder garantizar la continuidad de las operaciones de GNN7 TV.

Ejecución de pruebas reales del plan de contingencia.

Es necesaria la ejecución de pruebas reales de todo aquello que se ha establecido dentro del plan de contingencia. La facilidad de hacer pruebas parciales no debe impedir realizar pruebas exhaustivas ya que el propósito de estas últimas es poder determinar el alcance y efectividad del plan de contingencia actual. La prueba real contemplará lo siguiente:

- Verificación de que la información del plan es correcta y completa.
- Evaluación del personal involucrado.
- Evaluación de la coordinación entre el equipo de contingencia.
- Evaluación de la capacidad de recuperación.
- Evaluación de rendimiento general de GNN7 TV luego de la recuperación.

Elaboración del manual de contingencia

En este punto la organización sabe cuáles son sus procesos y sistemas críticos, conoce el impacto que supondría en su actividad el fallo de alguno de ellos. Tiene en su poder un conjunto de recomendaciones y buenas prácticas con el objetivo de evitar, en lo posible, desastres o interrupciones, es por esto que sabe cómo actuar en caso de

desastre y conocer el grado de responsabilidad de cada persona dentro de GNN7 TV; la organización se encuentra concienciada y con recursos económicos, que permitirán llevar a cabo ciertas pruebas en entornos reales.

Con todo este conocimiento, es el momento de elaborar el manual de contingencia que será la documentación de lo expuesto anteriormente, lo cual deberá ser escrito en un lenguaje simple capaz de ser entendido por el personal para lo cual no puede faltar la siguiente información:

- Situación previa al desastre.
- Cómo declarar una situación de desastre.
- Una identificación de procesos y recursos de TI que se deben recuperar.
- Identificación clara de responsabilidades.
- Plan de acción.
- Lista detallada de los recursos requeridos para la recuperación y continuidad del negocio.

Retroalimentación del plan de acción

Las empresas evolucionan y con ellas los procesos de negocio, lo que hoy es crítico para la continuidad de la empresa, mañana puede ser de escasa utilidad, por ello es necesario una continua revisión de los planes establecidos. Se deberán actualizar aquellos puntos que puedan cambiar o evolucionar a partir de la última revisión del plan de contingencia. Se recomienda establecer un cronograma para las revisiones y mantenimientos periódicos, todo ello asesorado por el personal que esté relacionado con las áreas a tratar. Para el buen mantenimiento de un plan de contingencia hay que tener en cuenta los siguientes puntos:

- Si cambian las necesidades del negocio, la estrategia que era adecuada puede pasar a no serlo.
- Pueden desarrollarse o adquirirse nuevas aplicaciones.
- Los cambios en las estrategias de negocio pueden cambiar la importancia de las aplicaciones críticas o hacer que se consideren críticas aplicaciones que antes no lo eran.

3.4.3.2 Política para respaldo y copias de seguridad de la información

Esta política tiene como propósito proporcionar directrices para el establecimiento de procedimientos de copia de seguridad e indicar lineamientos que especifiquen la forma de efectuar respaldo de la información general y copia de seguridad de servidores principales y secundarios para GNN7 TV. El área de TI requiere efectuar copias de seguridad periódicamente de los sistemas informáticos y que los medios de copia de seguridad se guarden en un lugar seguro fuera del sitio donde se encuentren. El propósito de la copia de seguridad de los sistemas es proporcionar un medio para:

- Restaurar la integridad de los sistemas informáticos en el caso de un fallo de hardware/software o desastre físico.
- Proporcionar una medida de protección contra el error humano o de la eliminación accidental de archivos importantes.
- Las copias de seguridad de sistemas consistirán en copias de seguridad completa y regularmente incremental.
- Las copias de seguridad de los sistemas se llevarán a cabo en un horario regular según lo determinado por el departamento de TI y se almacenarán en un lugar seguro, el cual puede ser “Google Drive” o localmente “Tivoli FastBack IBM”.
- El área de TI debe definir las directrices sobre la información que debe ser respaldada, dado el caso que los archivos de mayor importancia pueden ir desde los archivos administrativos creados en Microsoft Word, Excel y Power

Point hasta el almacenamiento de archivos multimedia dependiendo de los diferentes casos.

- El área de TI debe llevar a cabo una campaña informativa a los usuarios sobre los lineamientos y bajo qué circunstancias se realizará el respaldo dejando así por sentado (vía correo y de manera verbal) los archivos y directorios que van a ser respaldados.
- Es responsabilidad del área de TI la administración, revisión y gestión de los respaldos de información; ya sea de un servidor hasta una estación de trabajo.

Las excepciones a la política se permitirán siempre y cuando se justifiquen. Todas las excepciones deben estar completamente documentadas. El procedimiento estándar para los sistemas de copia de seguridad son los siguientes:

- Los usuarios deben efectuar copias de seguridad manuales de la información importante para la GNN7 TV ingresando a la página "Google Drive" (https://docs.google.com).
- Una copia de seguridad completa de los sistemas se realizará automáticamente cada vez que se detecten cambios en el equipo, este sistema de respaldo se encuentra instalado en todos los ordenadores de GNN7 TV.
- Las copias de seguridad se guardarán durante un año, momento en el que se pueden reciclar o destruir los medios de comunicación.
- Establecer controles ambientales adecuados, protección de temperatura, la humedad y el fuego, se mantendrán en el lugar de almacenamiento. Todos los medios de copia de seguridad que no son reutilizable serán destruidos completamente de una manera apropiada. Hacer copias de seguridad que se utilicen para otros fines serán borradas completamente.
- Pruebas y revisiones periódicas de las copias de seguridad se llevan a cabo para determinar si los archivos se pueden restaurar.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta. Corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red de GNN7 TV y que no estén previstas en las políticas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.4.4 Objetivo de Control - Gestión de la seguridad de las redes

OBJETIVO: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte. La gestión segura de las redes, la cual puede abarcar los límites organizacionales requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección, también se pueden requerir controles adicionales para proteger a la información que pasa a través de redes públicas.

3.4.4.1 Auditoria - Control de la Red

Objetivo

El objetivo de este control es que la red de GNN7 TV sea adecuadamente manejada y controlada para poder proteger la información y mantener la seguridad de los sistemas, aplicaciones y la red en general, incluyendo la información en tránsito.

Alcance

El alcance de este documento es que el departamento de TI implemente y optimice controles de red para así garantizar la seguridad de la información y proteger los servicios empresariales de accesos no autorizados.

Auditoria

Luego de hacer la respectiva auditoría se pudo observar que GNN7 TV no cuenta con correctas políticas de seguridad establecidas sobre la red, esto incluye que no posee una óptima arquitectura de red para así segmentar la seguridad por departamentos. Para los protocolos de comunicación que utilizan los diferentes servicios de GNN7 TV no existen controles de ningún tipo (Ejem.: ftp, smtp, sftp, pop, telnet, ssh). Se encontró que no existen restricciones o políticas de red entre host, redes y subredes (ACLs), todo el tráfico entre ellos está permitido.

GNN7 TV no cuenta con un dispositivo cortafuegos que haga cifrado o limite conexiones entrantes y salientes, tampoco existen políticas de seguridad de este tipo; la herramienta utilizada para hacer el filtrado de contenido web no funciona correctamente, esto otorga permisos de navegación a páginas no autorizadas.

No se controla adecuadamente a los dispositivos conectados a la red, esto incluye la no implementación del control de acceso a la red por dirección MAC para cada dispositivo. El departamento de TI no tiene implementados mecanismos de monitoreo general de la red.

Recomendaciones

Para que el departamento de TI pueda gestionar correctamente la red se deben considerar los siguientes puntos:

- Dividir la responsabilidad operacional de la red de GNN7 TV entre los miembros del departamento.
- Establecer responsabilidades y procedimientos para la gestión de las estaciones de trabajo.
- Aplicar un control de ingreso y monitoreo para permitir el registro de las acciones de seguridad relevantes.

- Establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasa a través de las redes públicas o a través de las redes inalámbricas; también se pueden requerir controles especiales para mantener la disponibilidad de los servicios de la red y computadoras.
- Las actividades de gestión deben ser comunicadas y coordinadas para optimizar el servicio a la organización y asegurar que los controles sean aplicados permanentemente.

3.4.4.2 Procedimiento para controles de red

La red de GNN7 TV debe estar correctamente administrada para poder proteger la información y mantener la seguridad de los sistemas, aplicaciones y la red en general, incluyendo la información en tránsito. El departamento de TI debe implementar controles para garantizar la seguridad de la información en la red, y proteger los servicios empresariales de accesos no-autorizados.

Jefe de tecnologías de la información / Coordinador de infraestructura y redes

Definir privilegios de cada usuario: Asegurar que los usuarios tienen el nivel de privilegio adecuado para las tareas que deben realizar, y reducir al mínimo el número de usuarios con nombres y contraseñas de administrador.

Descarga de archivos sólo de sitios de confianza: Asegurar que las descargas de contenido se limiten a sitios de confianza, restringir descargas desde sitios web de intercambio de archivos o sitios genéricos. Limitar los permisos de descarga a aquellos que lo necesitan hacer y capacitarlos para que lo hagan de forma segura.

Auditoría de recursos compartidos en la red: Eliminar unidades compartidas innecesarias y proteger las que estén en uso, esto con el fin de evitar que programas dañinos se propaguen a través de la red interna.

Vigilar conexiones de red: Monitorear las redes cuyo radio de cobertura alcancen las instalaciones de GNN7 TV para evitar que los ordenadores adopten configuraciones de redes no seguras y evitar infiltración de código malicioso o intrusos.

Modificar el rango de direcciones IP: Para las redes que aún utilizan rangos de direcciones IP estándar, como 10.1.x.x o 192.168.x.x. cambiar el rango IP predeterminado. Agregar reglas de cortafuegos como precaución adicional para permitir la conexión sólo a usuarios autorizados.

Controlar puertos abiertos de la red, bloquear los que no se utilicen: Limitar los puertos que permanecerán abiertos y limitar el tiempo que lo estarán, esto disminuirá el riesgo de que penetren la red personas no autorizadas, troyanos y/o gusanos. Es recomendable realizar una revisión periódica de todos los puertos.

Controlar periódicamente los puntos de acceso a su red: Supervisar todas las rutas que permiten conectarse a GNN7 TV (puntos de red, conexiones inalámbricas, equipos que permitan conexiones remotas, etc). Encontrar la forma de asegurar cada ruta de acceso para impedir que aplicaciones no solicitadas se introduzcan sin ser detectados.

Colocar los sistemas más importantes en una red distinta: Colocar estos sistemas en un segmento de red distinto de la red empleada para las actividades diarias.

Probar nuevas aplicaciones en redes virtuales: Para garantizar que las instalaciones o actualizaciones no causen problemas, primero realizar pruebas en un sistema virtual.

Desactivar los puertos USB no utilizados: Desactivar todos los puertos que no se utilicen, los puertos USB son una puerta abierta para que se infiltren programas maliciosos en la red ya que estos se ejecutan automáticamente al ser conectados.

3.4.4.3 Auditoria - Seguridad de los servicios de red

Objetivo

El objetivo de este control es que todos los servicios de red sean monitoreados periódicamente para garantizar su correcto funcionamiento y buen uso.

Alcance

El alcance de este control es que todos los equipos que forman parte de la infraestructura de red sean parte del sistema de seguridad implementado por el departamento de TI para así evitar fugas de información, acceso de terceros no autorizados y además garantizar su correcto funcionamiento y su buen uso.

Auditoria

- No hay control regular de los recursos informáticos que forman parte de la red.
- No se tienen plenamente identificadas las necesidades de seguridad de informática e información en GNN7 TV.
- GNN7 TV no tiene cortafuegos para gestionar y administrar el tráfico en la red.
- Cuenta con herramientas de protección contra malware en las estaciones de trabajo, pero no cuenta con una solución de seguridad eficaz.

Recomendaciones

- Se recomienda determinar y monitorear regularmente la capacidad de los servicios de red para así poder manejarlos de forma segura.
- Se recomienda identificar las políticas de seguridad necesarias para cada servicio de la red, características de seguridad, niveles de servicio y requerimientos de gestión. El departamento de TI debe garantizar la implementación de todos estos servicios.

- Los servicios de red incluyen la provisión de conexiones, servicios de redes privadas, soluciones de seguridad de red como cortafuegos y sistemas de protección contra malware o terceros no autorizados.

3.4.5 Objetivo de Control - Supervisión

OBJETIVO: Detectar las actividades de procesamiento de información no autorizadas. Se deben monitorear los sistemas, reportar eventos de seguridad de la información, utilizar bitácoras de operador y registrar fallas para asegurar que se identifiquen los problemas en los sistemas de información. La organización debe cumplir con los requerimientos legales relevantes a sus actividades de monitoreo y registro. Se debe utilizar el monitoreo del sistema para chequear la efectividad de los controles adoptados y verificar la conformidad con un modelo de política de acceso.

3.4.5.1 Auditoria - Registro de auditoría

Objetivo

El objetivo de este control es que se deben producir registros de actividades y eventos de seguridad de la información durante un período determinado y que ayuden en investigaciones futuras o auditorías del departamento de TI.

Alcance

El alcance de este control es que todas las actividades y eventos de seguridad de la información dentro de GNN7 TV generen registros que ayuden al departamento de TI para realizar futuras investigaciones y auditorías.

Auditoria

El departamento de TI no cuenta con un historial de incidentes, tampoco con una base de datos de conocimientos sobre problemas y soluciones para cada uno de los eventos ocurridos en los sistemas de información e informáticos de GNN7 TV.

La tarea de registro de incidentes no cuenta con un responsable, tampoco ningún miembro del departamento de TI documenta los incidentes que atendió. No se ha definido en los procedimientos internos del departamento de TI la tarea de registro de eventos o incidentes, no se realiza una correcta documentación de los mismos.

Recomendaciones

Se recomienda incluir registros que faciliten auditorías para todas las actividades y eventos del SGSI, además de los procedimientos realizados por el departamento de TI:

- Fechas, horas y detalles de eventos claves; por ejemplo, ingreso y salida.
- Ubicación de activos o lugar donde se realiza cada procedimiento.
- Registros de intentos de acceso fallido y exitoso a los datos y otros recursos.
- Cambios en la configuración del sistema.
- Uso de privilegios.
- Uso de las utilidades y aplicaciones del sistema.
- Archivos a los cuales se tuvo acceso y los tipos de acceso.
- Direcciones y protocolos de la red.
- Alarmas activadas por el sistema de control de acceso.
- Activación y desactivación de los sistemas de protección.

3.4.5.2 Auditoria - Registros de administrador y operador

Objetivo

El objetivo de este control es que se registren las actividades de los administradores del sistema y los operadores del sistema durante un período determinado para así tener un mayor control del SGSI y ayudar a investigaciones futuras o auditorías.

Alcance

El alcance de este control es que todas de las actividades de los administradores del sistema y los operadores del sistema generen registros que ayuden a tener un mayor control del SGSI, a futuras investigaciones y auditorías.

Auditoria

El departamento de TI no cuenta con un historial de actividades de los administradores y operadores del sistema, tampoco con una bitácora de los eventos o incidentes de seguridad de la información o informáticos en los que estuvo involucrado.

La tarea de registro de actividades no está definida como procedimiento dentro de las responsabilidades de cada uno de los miembros del departamento de TI.

Recomendaciones

Se recomienda incluir registros que faciliten la auditoría en todos los procedimientos realizados por el departamento de TI, los registros debieran incluir:

- La hora en que ocurre cada evento (éxito o falla).
- Toda la información relacionada a cada evento, por ejemplo: archivos manejados, el error ocurrido y la acción correctiva.
- Qué cuentas y procesos están involucradas en el evento, incluidos operador y/o administradores.

Los registros de administrador y operador del sistema debieran ser revisados de manera regular.

3.5 Dominio - Control de acceso

3.5.1 Objetivo de Control - Requisitos para el control de acceso

OBJETIVO: Controlar el acceso a la información. Se debiera controlar el acceso a la información, medios de procesamiento de la información y procesos comerciales sobre la base de los requerimientos comerciales y de seguridad. Las reglas de control del acceso debieran tomar en cuenta las políticas para la divulgación y autorización de la información.

3.5.1.1 Auditoria - Política de control de acceso

Objetivo

El objetivo de este control es identificar, documentar, revisar e implementar políticas de control de accesos generales a los sistemas de información e informáticos de la organización asegurando así procesos eficientes de auditoría y seguridad informática y del negocio.

Alcance

El alcance de este control es establecer políticas de gestión y buenas prácticas para el control de acceso a los diferentes sistemas de información. Esta política se aplica a todos los usuarios que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información de la organización que residen en servidores o sistemas locales y que tengan derechos de acceso a la información que puedan afectar los activos de información de la Organización.

Auditoria

GNN7 TV actualmente cuenta con diferentes sistemas de información para los cuales no existen procedimientos establecidos de gestión de acceso a los mismos, provocando con eso posibles accesos no autorizados, registrados, controlados ni gestionados a los sistemas de información.

Recomendaciones

- Todos los accesos a los sistemas informáticos se deben regir a la "Política de control de acceso" teniendo en cuenta que la misma debe ser cumplida para asegurar la eficiencia de los procesos de acceso sobre los sistemas informáticos y de información.
- Definir mecanismo de registro de acceso a los sistemas de información para así evitar accesos no autorizados a los mismos.
- Definir roles de accesos por usuarios con los respectivos permisos de configuración o cambios sobre los sistemas de información.
- El método más acertado para la gestión y control de acceso a los sistemas de información de la organización es el método conocido como RBAC, que permite definir roles en base a permisos, pudiendo así asignar usuarios a dichos roles dependiendo de las necesidades y funciones laborales dentro de la organización.
- Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- Identificar toda la información relacionada con las aplicaciones.
- Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de estaciones de trabajo.
- Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.
- Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la seguridad de la información.
- Establecer los niveles de acceso apropiados a la información institucional, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema y usuario.

3.5.1.2 Políticas de control de acceso

Las políticas detalladas a continuación deben ser acatadas por todo el personal de GNN7 TV, tomando en cuenta que los accesos a los diferentes sistemas de información e informáticos y sus procesos deben ser registrados, controlados y gestionados por el área de TI de la organización. La División Informática establece como Política de Control de Acceso el controlar el acceso a la información, a las instalaciones de procesamiento de la información (Datacenter) y a los procesos de provisión, los cuales deberán ser controlados sobre la base de los requisitos y seguridad. Para ello, a través de sus diferentes áreas de Operaciones, Software, Seguridad y Soporte permitirá administrar el ciclo de vida de los usuarios, desde la creación automática de las cuentas, roles y permisos necesarios hasta su inoperancia; a partir de los requerimientos reportadas por el departamento de Recursos Humanos y/o directamente de su Jefatura directa; lo anterior para que el funcionario tenga acceso adecuado a los sistemas de información y recursos tecnológicos, validando su autenticación, autorización y auditoría. GNN7 TV cuenta con sistemas computacionales que proporcionan servicios generales a la organización y son:

- Sistema de automatización de salida al aire
- Sistema de servidores de K2 para canales HD y SD
- Sistema centralizado de edición audio y video XSAN
- Sistema de Windows Server Active Directory
- Sistema de control y monitoreo de contenido web
- Sistema de impresiones centralizado
- Sistema de Respaldos
- Sistema de control de dispositivos de almacenamiento
- Sistema centralizado de despliego de políticas de actualización de software.

Los Sistemas de Información de GNN7 TV deben disponer de los mecanismos necesarios que permitan validar todos los usuarios en el momento de su conexión. Por lo tanto, no se permitirá la existencia de sistemas de información que no puedan identificar el usuario mediante un proceso lógico. Se debe garantizar lo siguiente:

- Cada usuario, dispondrá de un identificador único que pueda ser reconocido por los sistemas de información de la organización.
- A cada identificador de usuario corresponderá solo una persona física y tal esta estará autorizada a utilizarlo.
- Todas aquellas operaciones realizadas por un usuario, serán siempre imputadas al identificador utilizado que se hubiere identificado ante el sistema de información, independientemente de la persona física que lo haya realizado.

El procedimiento de generación de identificadores de usuario para los sistemas de información de la organización deberá, al menos, cumplir, siempre que técnicamente sea posible, con los siguientes requisitos mínimos:

- El código generado para este requisito debe proveer una identificación única.
- El procedimiento de generación, garantizará la imposibilidad de reasignar o reutilizar identificadores de usuario previamente utilizados.
- El procedimiento de generación garantizará la no duplicidad de los mismos.
- El procedimiento, garantizará que se cumpla con las reglas de identificación y nomenclatura, así como demás estándares aplicables.
- Se debe establecer una nomenclatura de usuarios para el caso de personal externo, así se identificará fácilmente si un usuario es parte de GNN7 TV.
- Será responsabilidad de los administradores del área de TI la implementación y gestión del mismo.

Este procedimiento, con ayuda del sistema informático de administración de usuarios, deberá exigir para generar un alta válida de usuario como mínimo, el cumplimiento y registro de los siguientes datos:

- Nombre y apellidos del usuario
- Número de empleado o identificación válida
- Departamento al que pertenece el usuario
- Tipo de usuario (interno, externo, genérico)
- Identificador asignado
- Fecha de alta
- Detalle de los permisos concedidos
- Fecha de inicio de creación del usuario

Siempre que sea técnicamente posible, se debe automatizar el procedimiento de bloqueo de identificadores de usuario, en los casos que se refieren a continuación, y según la clasificación de los sistemas o el perfil de las cuentas afectadas. Dichos procedimientos de bloqueo, se podrían ejecutar en los siguientes casos:

- Por caducidad de los identificadores de usuario.
- Por inactividad de los identificadores de usuario.
- Por intento de acceso fallido, utilizando dicho identificador en más de cinco intentos fallidos dependiendo del sistema al que se quiera acceder.
- Por baja temporal.
- Por baja definitiva (lo cual implicará la eliminación del identificador de usuario).

Para que exista un correcto control, el acceso a los recursos (ficheros, aplicaciones, bases de datos, sistema operativo, configuración, etc.) debe ser autorizado por los propietarios de los recursos o mediante una solicitud de acceso a los sistemas computacionales dirigida al área de TI. (Ver anexo #9). Las solicitudes de autorización, serán ejecutadas por los administradores de dichos recursos y el área de TI siguiendo las normativas impuestas por cada Responsable.

Como regla general, los usuarios únicamente tendrán acceso a los recursos necesarios para el ejercicio de sus funciones. Cualquier otro requerimiento al respecto se tramitará con el proceso de solicitud de acceso a los sistemas computacionales antes mencionada. Independientemente del tipo de acceso, interno o externo, dicho acceso debe ser autorizado previamente por el área de TI o propietario/responsable del recurso.

Los usuarios que requieran acceder a los recursos de los sistemas de información deberán seguir las siguientes pautas:

- El Responsable o Jefe de área de cada usuario, solicitará su requerimiento, mediante una solicitud de autorización (Ver anexo #9) con al menos los siguientes datos:
    - Nombre y apellidos del solicitante.
    - Fecha.
    - Sistemas a los que se solicita el acceso, así como el acceso requerido a cada uno.
    - Motivo de solicitud.
    - Autorización del propietario del recurso
    - Fecha límite de acceso al recurso (para casos de proveedores o consultores externos)

- El área de TI procesará la solicitud cumpliendo las siguientes reglas:
    - Verificar que las solicitudes de acceso a los sistemas computacionales cumplan con los requisitos necesarios mencionados con anterioridad.
    - Comprobar que la solicitud y asignación de perfiles, no interfiere con la Política de Seguridad o esquema de segregación de funciones establecidas.

Será responsabilidad de los administradores de sistemas ejecutar solamente aquellas solicitudes que hayan sido autorizadas de acuerdo a los que se indica en el apartado anterior de este procedimiento. En ningún caso asignarán privilegios y accesos a usuarios sin una solicitud previa.

Deberán resguardar todas las solicitudes tramitadas, y las pondrán a disposición en caso de auditorías internas o externas, así como para el control interno. En el caso de que se autorice el acceso a recursos por un tiempo determinado, el área de TI deberá cuidar que éste se cumpla, eliminando los privilegios en el tiempo establecido.

El área de TI debe garantizar el cumplimiento de los siguientes puntos para la posterior entrega a los usuarios de cualquier tipo de acceso a los sistemas computacionales de la organización, dichos aspectos a consideran son:

Usuario/Contraseña

Adoptar una política adecuada de contraseñas para validación o autenticación de usuarios, es el primer y más importante control para evitar los accesos no autorizados, o utilización indebida de los usuarios de los sistemas de información de la organización. Por ello, se debe elaborar una Política de Seguridad de la Información de obligado cumplimiento.

Se deberá cumplir, mediante el establecimiento de medidas automatizadas, las siguientes reglas de aplicación en la generación y utilización de contraseñas:

- Las contraseñas deberán tener una longitud mínima de x caracteres alfanuméricos (alfabéticos, numéricos y especiales, como por ejemplo %$&/()”!). La longitud depende de la importancia de la información protegida, normalmente de 8-12 caracteres.
- Cuando el usuario se identifique por primera vez en el sistema, éste deberá forzarle a realizar un cambio de su contraseña.
- Mediante el registro y conservación de un histórico de contraseñas por usuario, el sistema informático impedirá la utilización, al menos, de las últimas contraseñas.
- El usuario podrá realizar el cambio de su contraseña siempre que lo considere necesario.
- Ante un cambio de contraseña, el sistema informático solicitará la última contraseña con objeto de validar la misma.
- Las contraseñas caducarán de forma automática cada “x” días como máximo, y cumplido dicho plazo, el sistema obligará al usuario a cambiar su contraseña. La periodicidad marcada depende del nivel de información protegida.
- Un usuario quedará bloqueado al cabo de x intentos de acceso fallidos. Esta medida protege al sistema frente a ataques de fuerza bruta o muchos intentos fallidos. El número de intentos suele estar entre 5-8.
- El sistema, al cabo de x minutos de inactividad, realizará el bloqueo del terminal de usuario, exigiendo nuevamente la validación de la contraseña.
- Al cabo de x días como máximo de inactividad del identificador del usuario, éste quedará automáticamente bloqueado. Esta medida protege al sistema de usuarios que ya no deben tener acceso por haber causado baja.

Certificados

Existe la posibilidad de que los usuarios se identifiquen en el servidor mediante la presentación de un certificado. Los certificados de cliente normalmente contienen información como su nombre, organización, departamento, dirección de correo, ciudad, país, etc., lo que permite establecer mecanismos de autenticación y control de acceso más complejos, utilizando uno de estos atributos o en un conjunto de ellos.

La forma de uso es fácil e intuitiva, ya que el usuario simplemente instala el certificado en su sistema y posteriormente, cuando se conecte al servidor, sólo tiene que presentarlo para que se produzca la autenticación. Los certificados pueden almacenarse localmente en el disco duro del ordenador del usuario o en una tarjeta inteligente. En ambos casos, se encontrarán protegidos por una contraseña, para evitar el acceso fraudulento a los mismos.

Los certificados de usuarios, emitidos por una Autoridad de Certificación, pueden emplearse para uso internos, pudiendo emplear para ello una Autoridad de Certificación propia.

Los sistemas operativos Microsoft Windows Server y Linux incluyen servicios de certificación que permiten a las organizaciones emitir sus propios certificados.

Asignación de permisos, perfiles y roles

Los usuarios que acceden a los sistemas de información de la organización pertenecerán a un tipo de usuario determinado de acuerdo al rol o funciones que tenga en la organización.

A continuación se listan los perfiles de usuario más comunes que están presentes en una organización:

- Usuarios internos: serán todas aquellas personas que sean empleados de la organización.

- Usuarios externos: serán aquellos que estén adscritos o pertenezcan a un tercero que no es de la organización y que estén autorizados a conectarse a los sistemas de información de su propiedad.

- Usuarios genéricos: Como excepción a las normas generales descritas, y de manera autorizada por el Jefe del área designado podrán definirse y utilizarse usuarios genéricos.

Responsabilidad

Responsable de seguridad informática estará a cargo de:

- Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido.

- Definir pautas de utilización de Internet para todos los usuarios.

- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático y validarlos periódicamente.

- Controlar la asignación de privilegios a usuarios.

- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.

- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registro de usuarios y privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios, uso controlado de

utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de ruteo de red, etc.

- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
- Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:
    - Definir las actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión.
    - Determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.
- Definir un cronograma de depuración de registros de auditoría en línea.

Los propietarios de la información junto con la unidad de auditoría interna o en su defecto quien sea propuesto por el comité de seguridad de la información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades. El responsable de los departamentos y el responsable de

seguridad informática autorizarán el trabajo remoto de su personal, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información de modo de cumplir con las normas, también autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red e Internet. El responsable del área informática cumplirá las siguientes funciones:

- Implementar procedimientos para activación/desactivación de accesos a la red.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Evaluar el costo y el impacto de la implementación de los enrutadores adecuados para subdividir la red y recomendar el esquema apropiado.
- Implementar el control de puertos de conexión a la red y protocolos de red.
- Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como su depuración.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios.
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

La unidad de auditoría interna o en su defecto quien sea propuesto por el comité de seguridad de la información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad. El comité de seguridad de la información aprobará el análisis de riesgos efectuado y el período definido para el mantenimiento de los registros de auditoría.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta. Corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red de GNN7 TV y que no estén previstas en las políticas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.5.1.3 Formulario de registro de los accesos de usuarios

Utilizando este formato se podrá llevar un registro de los accesos otorgados a los usuarios de los sistemas de GNN7 TV.

FORMATO DE REGISTRO DE ACCESOS OTORGADOS A LOS USUARIOS								
Nombre	Apellido	Departamento	Jefe inmediato	Tipo de contrato	Sistema	Correo electronico	Sistema de edicion	Fecha de peticion

Figura #**3.49**: Formulario de registro de los accesos de usuarios

Elaborado por: Autores

3.5.2 Objetivo de Control - Gestión de acceso de usuario

OBJETIVO: Asegurar el acceso del usuario y evitar el acceso no autorizado a los sistemas de información. Se debieran establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información. Los procedimientos debieran abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta el des-registro final de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Cuando sea apropiado, se debiera prestar atención especial a la necesidad de controlar la asignación de derechos de acceso privilegiados, lo que permite a los usuarios superar los controles del sistema.

3.5.2.1 Auditoria - Registro de usuario

Objetivo

El objetivo de este control es establecer y garantizar procedimientos formales de alta y baja de usuarios con objeto de garantizar y cancelar los accesos y servicios de información y así impedir los accesos no autorizados a los sistemas informáticos y de información de la organización.

Alcance

El alcance de este control es establecer políticas de gestión y buenas prácticas para el control de acceso a los diferentes sistemas de información de la organización reservando el derecha de la organización de decidir la modalidad de registro de los accesos a cada uno de sus recursos, así como la posibilidad de adoptar nuevas modalidades de registros de acceso o suprimir otras. El modo en que se registra algún incidente sobre un recurso concreto debe acogerse a la normativa específica de uso.

Auditoria

Actualmente GNN7 TV no cuenta con el registro apropiado sobre cualquier incidencia reportada nivel de acceso de los usuarios a los sistemas informáticos de la

organización. El acceso a los recursos informáticos de GNN7 TV puede efectuarse de distintos modos:

- Por tener acceso al espacio físico (despacho, sala de ordenadores, zona de cobertura inalámbrica) en donde se encuentra el recurso (ordenador personal, servidor, punto de red, punto de acceso inalámbrico).
- A través de una cuenta de acceso de algún sistema de información (correo electrónico, cuenta de dominio, cuenta de acceso a servicios de red).

Recomendaciones

Todos los accesos a los sistemas informáticos y sus respectivos registros se deben regir a la "Política de registro de usuario" teniendo en cuenta que la misma debe ser cumplida para asegurar la eficiencia de los procesos de registros de accesos a los sistemas informáticos y de información.

Se deben establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información. Los procedimientos deberían cubrir todas la etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.

Se debería prestar especial atención, si fuera oportuno, a la necesidad de controlar la asignación de permisos de acceso con privilegios que se salten y anulen la eficacia de los controles del sistema.

Se deben tomar en consideración los accesos físicos a lugares restringidos donde residen equipos que almacenan información de vital importancia para la organización.

Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información cuando un usuario por diferentes razones no deba tener acceso a los sistemas computacionales. Se deben establecer procedimientos de registro de usuario, detallando en cada registro puntos como:

- Motivo de la solicitud de acceso
- Nombre del solicitante
- Jefe del solicitante
- Fecha de inicio y expiración del usuario con sus respectivas funciones

3.5.2.2 Política para el registro de usuario

Las políticas detalladas a continuación deben ser acatadas por todo el personal de GNN7 TV, tomando en cuenta que los accesos a los diferentes sistemas de información e informáticos y sus procesos deben ser registrados, controlados y gestionados por el área de TI de la organización.

El acceso y uso de determinados servicios y aplicaciones ofrecidas por GNN7 TV requiere ser registrada a través de un mecanismo de reportes sobre los incidentes relacionados a los accesos estos pueden ir desde fallos en la autenticación, cambios de claves, procesos de ejecución.

El área de TI debe establecer rutinas de auditoría de los registros de accesos de los usuarios a los diferentes sistemas de información de la organización para que así se mantenga vigilada la integridad y confiabilidad de los sistemas de información y que la información que maneja no sufra cambios provocados por accesos no autorizados a los mismos. (Ver 3.5.2.3).

Aspecto lógico de los registros de usuarios

El responsable de seguridad informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

- Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes debido a razones operativas.
- Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
- Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente.
- Entregar a los usuarios un detalle escrito de sus derechos de acceso.
- Requerir que los usuarios firmen declaración es señalando que comprenden y aceptan las condiciones para el acceso.
- Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
- Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la organización o sufrieron la pérdida/robo de sus credenciales de acceso.
- Efectuar revisiones periódicas con el objeto de:
    - Cancelar identificadores y cuentas de usuario redundantes.
    - Inhabilitar cuentas inactivas por un período mayor a 60 días.

    - Eliminar cuentas inactivas por un período mayor a 120 días.
    - En el caso de existir excepciones, deberán ser justificadas y aprobadas.
- Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
- Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o agentes intentan accesos no autorizados.
- Para acceder a determinados recursos de GNN7 TV (servicios y aplicaciones corporativas) es preciso disponer de una cuenta de acceso. Una cuenta de acceso consta de un identificativo de acceso (en adelante login) y de una clave de acceso (en adelante clave o contraseña). Una cuenta de acceso permite autenticar (identificar) a cualquier persona o entidad que pretenda acceder a cualquiera de los recursos informáticos corporativos.
- El área de TI en conjunto con el área de RRHH deciden cuáles de esos recursos puede usar esa persona o entidad.
- Las cuentas de acceso pueden ser personales o no personales. Las cuentas de acceso personales son para uso exclusivo del titular de la misma. Las cuentas de acceso no personales pueden ser usadas por más de una persona y están destinadas a permitir el acceso y compartir el uso de los recursos informáticos asociados a esa cuenta a un grupo de personas. El titular de una cuenta de acceso no personal es el responsable del grupo que hace uso de la misma.
- Una misma cuenta de acceso puede tener asociados uno o más recursos, de manera que el usuario de la cuenta puede acceder mediante el mismo login y contraseña a todos los recursos asociados a esa cuenta.

Normativa que, con carácter general, se aplican a las cuentas de acceso:

- Siempre debe haber una persona que responda del uso de una cuenta de acceso.
- El responsable de una cuenta de acceso personal es el titular de la misma.

- El responsable de una cuenta de acceso no personal es, en primer lugar, el titular de la misma y en segundo lugar los usuarios que comparten su uso.
- Solo el titular de una cuenta de acceso no personal puede cambiar su clave.
- Es responsabilidad del titular de la cuenta no personal el otorgar o revocar el uso de la misma a los usuarios que la comparten; el acto de otorgación o revocación se efectuara mediante el cambio de clave de la cuenta de acceso no personal y la posterior comunicación de la clave a aquellos usuarios que el titular estime conveniente.
- Es responsabilidad del titular de la cuenta no personal el registrar y documentar la otorgación o revocación sobre el uso de la cuenta a sus usuarios.
- La obtención de una cuenta de acceso compromete a su titular (y al resto de usuarios en el caso de cuentas no personales) a cumplir y hacer cumplir la normativa de uso general del presente documento así como la particular de los servicios a los que esa cuenta tenga acceso.
- Salvo cuentas de acceso no personales, no está permitido el uso de cuentas por personas ajenas a su titular (con conocimiento o no del mismo). Tampoco está permitido revelar la clave de una cuenta de acceso (salvo en el caso de cuentas de acceso no personales).
- Cualquier cambio en la titularidad de una cuenta de acceso debe ser comunicado inmediatamente al responsable administrativo correspondiente.
- No está permitido el uso de cuentas personales por otra persona que no sea el titular de la cuenta (con conocimiento o no del titular).
- No está permitido revelar la clave de una cuenta de acceso (salvo en el proceso de otorgación de uso de una cuenta de correo no personal).
- El usuario debe notificar inmediatamente al área de TI cualquier sospecha de uso no autorizado de una cuenta de acceso o de cualquier otro fallo de seguridad.
- Asimismo, el usuario debe asegurarse de que su cuenta queda cerrada al final de cada sesión, con el fin de que no pueda ser usado por terceras personas. Si

se produjera un mal uso de la misma bajo estas circunstancias, la responsabilidad es del citado usuario.

- El área de TI se reserva el derecho de aceptar o no la creación de cuentas. Asimismo, podrá suspender o cancelar cuentas por uso indebido, sin perjuicio de imponer las sanciones correspondientes.

Estados de las cuentas de acceso

Dada una cuenta de acceso y un recurso asociado a esa cuenta (por ejemplo el servicio de correo electrónico), se definen, con carácter general, los siguientes estados para la cuenta:

- Cuenta activa. Todas las funciones del recurso asociado a esa cuenta están disponibles (por ejemplo, recibir, enviar, leer o eliminar mensajes).
- Cuenta cancelada. El recurso asociado a esa cuenta ya no está disponible para el usuario de la cuenta (el usuario no puede usar el correo). Los datos del recurso asociados a esa cuenta pueden ser eliminados o movidos a un espacio de almacenamiento offline (por ejemplo, el buzón del usuario puede ser suprimido o movido a otro sitio).
- Cuenta bloqueada. El recurso asociado a esa cuenta tiene limitadas todas o parte de sus funcionalidades (por ejemplo no puede recibir mensajes, no puede enviar mensajes, si puede leer y borrar los ya existentes en su buzón).

Las cuentas de acceso se crean inicialmente en estado activas para los recursos asociados.

- Una cuenta de acceso puede ser bloqueada para todos o alguno de sus recursos asociados en alguno de los siguientes casos:

- Por decisión de la autoridad competente de GNN7 TV, al cometer el usuario de la cuenta una infracción lo suficientemente grave en el uso del recurso.

- Por motivos técnicos que aconsejen su bloqueo en situaciones de emergencia mientras duren procesos de mantenimiento del recurso o recursos asociados a la cuenta, mientras se rebasen los parámetros de funcionamiento del recurso por parte del usuario de la cuenta (por ejemplo se llena el buzón de correo)

- Una cuenta de acceso puede ser cancelada en los casos contemplados en el punto

    - Finalmente, una cuenta de acceso se elimina, desapareciendo todo rastro de la cuenta y de los datos de los recursos asociados si y sólo si lleva cancelada un periodo de tiempo determinado y específico para cada uno de los recursos asociados.

    - El login de una cuenta de acceso eliminada puede ser rehusado (puede ser asignado a otra cuenta de acceso nueva).

- Cada normativa específica de un recurso o servicio puede definir otros estados para las cuentas de acceso, así como modificar su significado.

Creación de cuentas de acceso

Para crear una cuenta de acceso personal el titular de la cuenta debe tener una relación formal y vigente con GNN7 TV, apareciendo sus datos de filiación en las bases de datos del sistema de RRHH. Esto es, la persona en cuestión pertenece al colectivo.

- En el caso de pertenecer de manera formal a la organización, se generará una cuenta de acceso de manera automática en el momento de establecer su relación con GNN7 TV (formalización del contrato).

- Esta cuenta otorga acceso a los recursos informáticos básicos que la autoridad competente del área de TI crea convenientes (por ejemplo, correo electrónico).

- Si por el motivo que fuese, un miembro de GNN7 TV no tuviese cuenta de acceso para acceder a los recursos informáticos básicos, podrá solicitarla en cualquier momento mediante los procedimientos habilitados al efecto al jefe del departamento de TI.

- Las personas que no pertenezcan a ninguno de los colectivos arriba mencionados y necesiten obtener una cuenta de acceso, podrán hacerlo mediante solicitud efectuada por el responsable de la unidad organizativa de la que dependen.

Cuentas de acceso no personales

- Para crear una cuenta de acceso no personal, ésta deberá ser solicitada por el responsable del grupo o unidad organizativa que va a usarla.

- El responsable del grupo debe pertenecer a GNN7 TV o estar debidamente autorizado por la autoridad competente. Una vez creada la cuenta de acceso el responsable que la solicitó pasa a ser el titular de la cuenta.

Procedimiento de creación de las cuentas de acceso y asignación de recursos

- Siempre que sea posible, la solicitud de creación de una cuenta de acceso se efectuará por medios informáticos, para ello el solicitante de la cuenta deberá acreditar su identidad mediante certificado digital personal.

- Cuando el solicitante no disponga de certificado digital y no pueda solicitar la cuenta por medios informáticos, la solicitud podrá efectuarse mediante formulario dirigido al are área de TI y debidamente sellado por el jefe de la unidad organizativa interesado en la creación de la cuenta. En este caso es responsabilidad del jefe de la unidad organizativa el comprobar la identidad del usuario de la cuenta cuando se trate de cuentas personales.

- Una vez comprobada la identidad del solicitante y el derecho a obtener la cuenta de acceso, se procederá a la creación de la cuenta. La creación de la cuenta puede postergarse por motivos técnicos justificados, en cualquier caso el área de TI informará al solicitante por los medios que considere más oportunos de:
    - Cuándo ha sido o será creada la cuenta
    - La clave de acceso a la misma.
    - Documentación relativa al uso de los servicios informáticos a los que la cuenta permite acceder: normativa específica de cada servicio, parámetros de configuración de cada servicio, etc.
- En el caso de que la solicitud sea rechazada se informará al solicitante de los motivos del rechazo.
- Los recursos y servicios informáticos básicos asignados a una cuenta de acceso pueden variar en función del colectivo al que pertenece el usuario o del tipo de cuenta (personal, no personal).
- Es la autoridad competente de GNN7 TV la que decide los recursos asociados a una cuenta de acceso en función del tipo y del colectivo al que va destinada.

Cancelación de cuentas de acceso

Con carácter general, se procederá a cancelar una cuenta de acceso cuando:

- En el caso de cuentas personales, la relación de la persona con GNN7 TV deje de estar vigente.
- El responsable de la cuenta solicita la cancelación de la misma.
- Por decisión de la autoridad competente por comisión de infracciones que lleven pareja la cancelación de la cuenta de correo.
- Cuando no se detecte actividad en el uso de la cuenta (abandonadas)

En cualquier caso será la autoridad competente del área de TI la que decida en qué casos, cuándo y cómo se cancela una cuenta de acceso, así como la de arbitrar excepciones a las normas de carácter general arriba expuestas.

Salvo indicación expresa de la autoridad competente de GNN7 TV, o causas de fuerza mayor, la cancelación de una cuenta de acceso será avisada con tiempo suficiente para que el responsable de la misma efectúe las acciones oportunas sobre cualquier dato almacenado en el recurso o recursos asociados a la cuenta de acceso. El aviso se efectuará mediante mensaje de correo electrónico o por cualquier otro medio que se estime oportuno.

Acceso al espacio físico

Para acceder a determinados recursos de GNN7 TV (ordenadores personales, servidores, puntos de red) hay que tener acceso al espacio físico en el que se encuentran. El acceso a este espacio físico puede ser restringido o abierto, en cualquier caso, es tarea del responsable administrativo pertinente controlar quién accede al espacio.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta. Corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red de GNN7 TV y que no estén previstas en las políticas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.5.2.3 Formulario de registro de usuarios

Utilizando este formato se podrá registrar la creación de los usuarios en los sistemas de GNN7 TV.

FORMULARIO DE REGISTRO DE INCIDENTES SOBRE LOS USUARIOS						
Nombre	Apellido	Departamento	Jefe de area	Incidente	Solucion	Comentarios

Figura #3.50: Formulario de registro de usuarios

Elaborado por: Autores

3.5.2.4 Auditoria - Gestión de privilegios

Objetivo

El objetivo de este control es limitar y controlar la asignación y uso de privilegios de acceso de los usuarios de la organización o externos a los sistemas informáticos y de información; el mal uso de los privilegios es una de las causas más frecuente y principales que contribuye a la falla de los sistemas informáticos y de información.

Alcance

Establecer políticas de gestión y buenas prácticas para el control de privilegios a los diferentes sistemas de información de la organización que requieren protección contra cambios provocados por usuarios con privilegios de administrador provocando así la inestabilidad de los servicios y posibles fallas de los sistemas de información.

Auditoria

Actualmente GNN7 TV no cuenta con una correcta gestión de asignación, documentación y gestión general de privilegios en la mayoría de sus sistemas informáticos y de información.

Recomendaciones

- Identificar los privilegios asociados a cada sistema informático y de información por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, accesos a Internet, etc.
- Asignar los privilegios basándose en su necesidad laboral, por ejemplo el requerimiento mínimo para su rol funcional dentro de la organización.
- Todos los accesos a los sistemas informáticos y su respectiva gestión de privilegios de usuario se deben regir a la "Política de gestión de privilegios" teniendo en cuenta que la misma debe ser cumplida para asegurar la eficiencia de los procesos de gestión de los mismos.
- Mantener un proceso de autorización y un registro de privilegios asignados.
- Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.
- Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios innecesarios.
- La asignación de privilegios debe ser controlada mediante un proceso de autorización formal que debe ser debidamente registrado y documentado para así conocer los privilegios de los usuarios no autorizados o autorizados a los sistemas información.

3.5.2.5 Política de la gestión de privilegios

Las políticas detalladas a continuación deben ser acatadas por todo el personal de GNN7 TV, tomando en cuenta que la asignación de privilegios a los diferentes sistemas de información e informáticos y sus procesos debe ser registrada, controlados y gestionados por el área de TI de la organización. El acceso y uso de determinados

servicios y aplicaciones ofrecidas por GNN7 TV requiere ser registrada a través de un mecanismo de reportes sobre los incidentes relacionados a los accesos debido a la incorrecta implementación de los privilegios de usuarios; estos pueden ir desde cambios en los servicios informáticos de la organización hasta manipulación de información.

El área de TI debe establecer rutinas de auditoría de revisión de los privilegios de gestión otorgados a los usuarios de la organización para que así se mantenga vigilada la integridad y confiabilidad de los sistemas de información y que la información que maneja no sufra cambios provocados por accesos no autorizados a los mismos. (Ver 3.5.2.6). Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

- Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
- Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados.
- Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización. (Anexo #10).

- Establecer un período de vigencia para el mantenimiento de los privilegios luego del cual los mismos serán revocados.
- Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.
- Los propietarios de información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el responsable de seguridad informática.
- Ningún usuario final debe tener privilegios de usuario administrador de algún sistema informático y de información.

Los administradores deberán tener dos cuentas en el sistema: una cuenta administrativa y una cuenta de usuario normal. Se debería utilizar la cuenta de usuario normal a menos que se estén realizando tareas administrativas. A causa de los privilegios asociados a las cuentas administrativas, son un objetivo primario para los intrusos.

- Revisar las asignaciones de privilegios cada mes, a fin de garantizar que no se obtengan privilegios no autorizados.
- Se deshabilitarán las cuentas creadas por ciertas aplicaciones con privilegios de sistema, (cuentas del servidor de aplicaciones, cuentas de herramientas de auditoría, etc.) evitando que estas corran sus servicios con privilegios nocivos para la seguridad del sistema.
- Todo servicio provisto o instalado en los servidores, correrá o será ejecutado bajo cuentas restrictivas, en ningún momento se obviaran situaciones de servicios corriendo con cuentas administrativas, estos privilegios tendrán que ser eliminados o configurados correctamente.
- Deberá autorizar el acceso a su información a toda persona o grupo que requiera. Este acceso contemplará los privilegios respectivos (lectura, escritura, actualización y eliminación).

- Cada aplicación debe gestionar el nivel de privilegios que tienen los usuarios dentro del sistema informático.
- Todo el personal de GNN7 TV debe estar asociado a un rol/perfil en los sistemas informáticos de acuerdo a las actividades que realiza.
- Es responsabilidad de los administradores de servidores y servicios, la correcta administración de las cuentas de acceso, el otorgamiento de privilegios de acuerdo a las autorizaciones que se especifiquen en el flujo de autorización.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta. Corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red de GNN7 TV y que no estén previstas en las políticas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.5.2.6 Formulario de registro de la gestión de privilegios

Utilizando este formato se podrá registrar todo lo relacionado a la gestión de privilegios de los usuarios de GNN7 TV.

FORMULARIO DE REGISTRO DE LA GESTION DE PRIVILEGIOS								
FECHA	NOMBRE	APELLIDO	DEPARTAMENTO	TIPO DE PRIVILEGIO	JEFE SOLICITANTE	JUSTIFICACION	OBSERVACIONES	SISTEMA

Figura #3.51: Formulario de registro de la gestión de privilegios

Elaborado por: Autores

3.5.2.7 Auditoria - Gestión de contraseñas de usuario

Objetivo

El objetivo de este control es establecer un estándar de control para la creación y asignación de contraseñas seguras, mediante un proceso de gestión formal.

Alcance

El alcance de este control es establecer políticas de gestión y buenas prácticas para la gestión de contraseñas de accesos a los diferentes sistemas de información de la organización que requieren protección contra accesos no autorizados y debe regirse bajo un estándar de creación formal de contraseñas que incluye a todo el personal que tienen o son responsables de una cuenta (o cualquier otra forma de acceso que admita o requiera contraseña) en cualquier sistema informático y de información de GNN7 TV que tenga acceso a la red corporativa o almacena cualquier información no pública de GNN7 TV.

Auditoria

Actualmente GNN7 TV cuenta con políticas de seguridad establecidas para la creación de contraseñas que a su vez mantiene formatos de complejidad, tiempo de validez y evita la configuración de contraseñas muy sencillas o fáciles de descubrir. Con lo que no cuenta es con un sistema integrado de control de la gestión de las contraseñas; esto quiere decir que cualquier incidente como cambio, pérdida o creación de claves no son registradas.

Recomendaciones

- Todos los accesos a los sistemas informáticos y su respectiva gestión de privilegios de usuario se deben regir a la “Política de gestión de privilegios” teniendo en cuenta que la misma debe ser cumplida para asegurar la eficiencia de los procesos de gestión de privilegios sobre los sistemas de la empresa.

- La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

- Se debe aplicar el estándar de creación de contraseñas seguras para el acceso de usuarios finales a los diferentes sistemas.

- Se debe aplicar el estándar de creación de contraseñas seguras para el acceso a la administración de los sistemas, servidores y los demás equipos de comunicación.

- No habilitar la opción "recordar clave en este equipo" que ofrecen los programas.

- No enviarla por correo electrónico.

- Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.

3.5.2.8 Política de gestión de contraseñas de usuario

Las políticas detalladas a continuación deben ser acatadas por todo el personal de GNN7 TV, tomando en cuenta que la gestión de contraseñas de acceso de usuarios a los diferentes sistemas de información e informáticos y sus procesos debe ser registrada, controlada y gestionada por el área de TI de la empresa.

El acceso y uso de determinados servicios y aplicaciones ofrecidas por GNN7 TV requiere ser registrada a través de un mecanismo de reportes sobre los incidentes relacionados a los accesos debido a la incorrecta implementación de la gestión de contraseñas de usuarios; estos pueden ir desde cambios en los servicios informáticos de la organización hasta manipulación de información.

El área de TI debe establecer rutinas de auditoría de revisión de los privilegios de la gestión de contraseñas de acceso de los usuarios de la organización para que así se mantenga vigilada la integridad y confiabilidad de los sistemas de información y que la información que maneja no sufra cambios provocados por accesos no autorizados a los mismos. Las contraseñas son un aspecto importante de la seguridad informática. Una contraseña mal elegida puede resultar en un acceso no autorizado y/o exploración de los recursos de GNN7 TV. Todos los usuarios, incluyendo contratistas y proveedores con acceso al sistema corporativo, serán responsables de tomar las medidas pertinentes, tal como se indica a continuación, para seleccionar y proteger sus contraseñas.

La siguiente política detalla la gestión de contraseñas a usuarios y que a su vez controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el compromiso de confidencialidad (Ver anexo #11).
- Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
- Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.
- Almacenar las contraseñas sólo en sistemas informáticos protegidos.

- Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el responsable de seguridad informática conjuntamente con el responsable del área de informática y el propietario de la información lo determine necesario (o lo justifique).

- Configurar los sistemas de tal manera que las contraseñas tengan (especificar cantidad no menor a 8 caracteres) caracteres

- Suspender o bloquear permanentemente al usuario luego de (especificar cantidad no mayor a 3) intentos de entrar con una contraseña incorrecta (deberá pedir la rehabilitación ante quien corresponda)

- Solicitar el cambio de la contraseña cada (especificar lapso no mayor a 45 días).

- Impedir que las últimas (especificar cantidad no menor a 12) contraseñas sean reutilizadas

- Establecer un tiempo de vida mínimo de (especificar cantidad no mayor a 3) días para las contraseñas.

Uso de contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. Los usuarios deben cumplir las siguientes directivas:

- Mantener las contraseñas en secreto.

- Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

- Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:
    - Sean fáciles de recordar.
    - No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
    - No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- Cambiar las contraseñas provisorias en el primer inicio de sesión ("log on").
- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.
- Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.
- Por ningún motivo personas ajenas a GNN7 TV podrán hacer uso de los equipos de cómputo pertenecientes a GNN7 TV. Es responsabilidad del custodio proteger el inicio de sesión del sistema operativo con contraseña, para que nadie pueda acceder al mismo.
- Está prohibido utilizar contraseñas en el BIOS del computador, pudiendo el departamento de TI eliminarlas, restableciendo el inicio normal del equipo.
- Todas las contraseñas de nivel de sistema (por ejemplo, root, enable, administrador de Windows, las cuentas de administración de aplicaciones, etc.) deben cambiarse por lo menos en una base trimestral.

- Todas las contraseñas a nivel de sistema deben ser administradas y gestionadas por el departamento de TI.
- Todas las contraseñas de nivel de usuario (por ejemplo, correo electrónico, web, computadores de escritorio, etc.) deben cambiarse por lo menos cada seis meses.
- Las cuentas de usuario que tienen privilegios de nivel de sistema a través de grupos o programas como “sudo” deben tener contraseñas únicas con respecto a las demás cuentas mantenidas por el usuario.
- Siempre use diferentes contraseñas para diferentes necesidades de acceso siempre que sea posible.
- No comparta las contraseñas con nadie, incluyendo asistentes administrativos o secretarias.
- Todas las contraseñas deben ser tratadas como sensibles y confidenciales.
- Las contraseñas nunca deben estar por escrito o almacenados en línea sin cifrado.
- No revelar una contraseña por el correo electrónico, chat o vía comunicación electrónica.
- No hablar de una contraseña en frente de otros.
- No insinuar el formato de una contraseña (por ejemplo, "nombre de mi familia").
- No revelar una contraseña en cuestionarios o formularios de seguridad.
- Si alguien pide una contraseña, que se refiere a este documento comunicarlo inmediatamente al departamento de TI.
- Siempre rechazar el uso de la "recordar contraseña" característica de las aplicaciones (por ejemplo, Gmail, Outlook, Netscape Messenger).

Directrices generales de construcción de contraseñas

Todo el personal deberá ser consciente de cómo seleccionar contraseñas seguras. Las contraseñas fuertes deben contener al menos tres de las cinco características siguientes:

- Caracteres en minúsculas.
- Caracteres en mayúsculas.
- Números.
- Puntuación.
- Caracteres "especiales" (por ejemplo, "@#$%^&*()_+|~-=\'{}[]:";'<>/, etc.)
- Contener al menos quince caracteres alfanuméricos.

Las contraseñas débiles tienen las siguientes características:

- Las contraseñas contienen menos de quince caracteres.
- La contraseña es una palabra que se encuentra en un diccionario (cualquier idioma).
- La contraseña es una palabra de uso común, tal como:
    - Nombres de familia, mascotas, amigos, compañeros de trabajo, personajes de fantasía, etc., términos o nombres de equipo, y comandos, sitios, empresas, hardware, software.
    - Las palabras "GNN7 TV", "sanjose", "sanfran" o cualquier derivación.
    - Los cumpleaños y otra información personal como direcciones y números de teléfono.
    - Palabras o números de patrones como aaabbb, qwerty, 123321, etc.

- Cualquiera de las anteriores deletreado al revés.
- Cualquiera de los anteriores precedido o seguido por un digito (por ejemplo, secret1, 1secret)

Trate de crear contraseñas que pueden ser fáciles de recordar, una forma de hacer esto es crear una contraseña basada en el nombre de una canción o frase. Por ejemplo, la frase podría ser: "Esta puede ser una manera de recordar", la contraseña sería "TmB1w2R" que utiliza la letra inicial de cada palabra de esta frase traducida al inglés.

Seguridad de aplicaciones

Los desarrolladores de aplicaciones deben garantizar que sus programas contienen las precauciones de seguridad siguientes:

- Crear autenticación para usuarios individuales, no grupos.
- No podrán almacenar las contraseñas en texto claro o en cualquier otra forma fácilmente visible.

Uso de contraseñas y frases de contraseña para los usuarios de acceso remoto

El acceso a la red empresarial a través de acceso remoto se controla utilizando la autenticación de contraseña o un sistema de clave pública y/o clave privada con una contraseña fuerte.

Frases de acceso

Las frases de acceso que se utilizan generalmente para la autenticación de clave pública y/o privada utilizan un sistema de relación matemática entre la clave pública que es conocida por todos, y la clave privada, que es conocido solamente por el usuario.

Sin la contraseña para "desbloquear" la clave privada, el usuario no puede tener acceso; las frases de acceso no son las mismas que las contraseñas. Una frase de acceso es una versión más larga de una contraseña y es, por lo tanto, más seguro. Una frase de acceso se compone típicamente de varias palabras. Debido a esto, una frase de contraseña es más segura contra los "ataques de diccionario". Una buena contraseña es relativamente larga y contiene una combinación de letras mayúsculas, minúsculas, caracteres numéricos y la puntuación. Todas las reglas anteriores que se aplican a las contraseñas se aplican también a las frases de acceso.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta; corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red de GNN7 TV y que no estén previstas en las políticas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.5.2.9 Formulario de registro de gestión contraseñas a usuarios

Utilizando este formato se podrá registrar todo lo relacionado a la gestión de contraseñas en GNN7 TV.

FORMULARIO DE REGISTRO DE GESTION DE CONTRASEÑAS DE USUARIOS								
FECHA	NOMBRE	APELLIDO	DEPARTAMENTO	JEFE DE AREA	SUCURSAL	FECHA DE CAMBIO DE CONTRASEÑA	MOTIVO	COMENTARIOS

Figura #3.52: Formulario de registro de gestión contraseñas a usuarios

Elaborado por: Autores

3.5.3 Objetivo de Control - Control de acceso al sistema operativo

OBJETIVO: Evitar el acceso no autorizado a los sistemas operativos. Se debieran utilizar medios de seguridad para restringir el acceso a los sistemas operativos a los usuarios autorizados.

3.5.3.1 Auditoria - Procedimientos seguros de inicio de sesión

Objetivo

El objetivo de este control es identificar, documentar, revisar e implementar procedimientos de inicio de sesión segura a los sistemas de información e informáticos asegurando así procesos eficientes de auditoría y seguridad informática y del negocio.

Alcance

El alcance de este control es establecer procedimientos seguros de gestión y buenas prácticas que permitan proporcionar una solución para controlar la conexión e inicio de sesión segura a los sistemas informáticos y de información de la organización.

Auditoria

GNN7 TV no cuenta con procedimientos de inicio de sesión seguro para la mayoría de sus sistemas de información, en algunos casos no están definidos usuarios con inicio de sesión única para almacenar registros generales sobre cambios o alteraciones a los sistemas informáticos de la organización y así con esto conocer de manera inmediata cualquier responsable por daños, pérdida o mala gestión de la información.

Recomendaciones

- Definir mecanismo de registro de inicio de sesión a los sistemas de información para así evitar accesos no autorizados a los mismos.
- El acceso al sistema operativo debe ser protegido con inicio de sesión seguro.

- Todos los accesos a los sistemas informáticos se deben regir a la "Política de procedimiento seguro de inicio de sesión" teniendo en cuenta que la misma debe ser cumplida para asegurar la eficiencia de los procesos de acceso sobre los sistemas informáticos y de información.

3.5.3.2 Políticas del procedimiento general de inicio de sesión

Las políticas detalladas a continuación deben ser acatadas por todo el personal de GNN7 TV, tomando en cuenta que el procedimiento seguro de inicio de sesión de usuarios a los diferentes sistemas de información e informáticos y sus procesos deben ser registrados, controlados y gestionados por el área de TI de la organización. El acceso y uso de determinados servicios y aplicaciones ofrecidas por GNN7 TV requiere ser registrada a través de un mecanismo de reportes (Ver 3.5.3.3) sobre los incidentes relacionados a los accesos debido a la incorrecta implementación de los procedimientos seguros de inicio de sesión; estos pueden ir desde cambios en los servicios informáticos de la organización hasta manipulación de información. El área de TI debe establecer rutinas de auditoría de revisión del procedimiento seguro de inicio de sesión de los usuarios de la empresa, para que así se mantenga vigilada la integridad y confiabilidad de los sistemas de información y que la información que maneja no sufra cambios provocados por accesos no autorizados a los mismos. A fin de mantener un control eficaz del acceso a los datos y servicios de información, el área de TI debe llevar a cabo un proceso formal, a intervalos regulares de un mes, a fin de revisar los derechos de acceso de los usuarios.

Para lo cual se deberán contemplar los siguientes controles:

- Revisar los derechos de acceso de los usuarios cada mes.
- Revisar las autorizaciones de privilegios especiales de acceso cada mes.
- Revisar las asignaciones de privilegios cada mes, a fin de garantizar que no se obtengan privilegios no autorizados.

- Se deshabilitarán las cuentas creadas por ciertas aplicaciones con privilegios de sistema, (cuentas del servidor de aplicaciones, cuentas de herramientas de auditoría, etc.) evitando que estas corran sus servicios con privilegios nocivos para la seguridad del sistema.

- Al terminar una sesión de trabajo en las estaciones, los operadores o cualquier otro usuario, evitará dejar encendido el equipo, pudiendo proporcionar un entorno de utilización de la estación de trabajo

El acceso a los sistemas operativos estará protegido, mediante un inicio seguro de sesión, que contemplará las siguientes condiciones:

- No mostrar información del sistema hasta que este haya iniciado.

- No suministrar mensajes de ayuda, durante el proceso de autenticación.

- Validar los datos de acceso cuando se han diligenciado los datos de entrada.

- Limitar el número de intentos fallidos de conexión registrando y auditando los intentos no exitosos.

- No mostrar las contraseñas digitadas.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta; corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red de GNN7 TV y que no estén previstas en las políticas, serán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.5.3.3 Formulario de registros de inicio de sesión

Utilizando este formato se podrá registrar los inicios de sesión e incidentes de cada usuario de GNN7 TV.

FORMULARIO DE REGISTRO DE INICIO DE SESION DE LOS USUARIOS									
NOMBRE	APELLIDO	USUARIO	DEPARTAMENTO	SISTEMA	TIPO DE INICIO	FECHA	HORA	INCIDENTES	OBSERVACIONES

Figura #3.53: Formulario de registros de inicio de sesión

Elaborado por: Autores

3.5.3.4 Auditoria - Identificación y autenticación de usuario

Objetivo

El objetivo de este control es identificar, documentar, revisar e implementar procedimientos generales para la identificación y autenticación de usuarios a los sistemas de información e informáticos de la organización asegurando así procesos eficientes de auditoría y seguridad informática.

Alcance

El alcance de este control es establecer procedimientos seguros de gestión y buenas prácticas que permitan proporcionar una solución para controlar la conexión e inicio de sesión segura a los sistemas informáticos y de información de la organización.

Auditoria

GNN7 TV no cuenta con procedimientos de inicio de sesión seguro para la mayoría de sus sistemas de información, en algunos casos no están definidos usuarios específicos con inicio de sesión única para almacenar registros generales sobre

cambios o alteraciones a los sistemas informáticos de la organización y así conocer inmediatamente al responsable por daños, pérdida o mala gestión de la información.

Recomendaciones

- Todos los accesos a los sistemas informáticos se deben regir a la "Política de identificación y autenticación" teniendo en cuenta que esta debe cumplirse para asegurar la eficiencia de los procesos de acceso a los sistemas de la empresa.
- Definir mecanismos de registro del proceso de identificación y autenticación de usuarios a los sistemas de información para evitar accesos no autorizados.
- El acceso a los sistemas operativos estará protegido, mediante mecanismos de identificación y autenticación de usuarios.
- Todos los usuarios deberían disponer de un único identificador propio para su uso personal y exclusivo. Se debería elegir una técnica de autenticación adecuada que verifique la identidad reclamada por un usuario.
- Cada sistema debe incorporar la autenticación de usuario y la identificación para garantizar que el acceso no se concederá a personas no autorizadas.
- Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single login" o sincronización de passwords.
- Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder.
- El servidor de autenticaciones no será necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

- La seguridad informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.

3.5.3.5 Política de identificación y autenticación de usuarios

Las políticas detalladas a continuación deben ser acatadas por todo el personal de GNN7 TV, tomando en cuenta que el procedimiento de identificación y autenticación de usuarios a los diferentes sistemas de información e informáticos y sus procesos deben ser registrados, controlados y gestionados por el área de TI de la organización.

El acceso y uso de determinados servicios y aplicaciones ofrecidas por GNN7 TV requiere ser registrada a través de un mecanismo de reportes sobre los incidentes relacionados a los accesos debido a la incorrecta implementación de los procedimientos de identificación y autenticación de usuarios; estos pueden ir desde cambios en los servicios informáticos de la organización hasta la incorrecta manipulación de información.

El área de TI debe establecer rutinas de auditoría de revisión del procedimiento de identificación y autenticación de usuarios de la organización para que así se mantenga vigilada la integridad y confiabilidad de los sistemas de información y que la información que maneja no sufra cambios provocados por accesos no autorizados a los mismos.

Se denomina identificación al momento en que el usuario se da a conocer en el sistema, y autenticación a la verificación que realiza el sistema sobre esta identificación. Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta

llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado. En circunstancias excepcionales, cuando existe un claro beneficio para la organización, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del propietario de la información de que se trate.

Si se utilizará un método de autenticación físico (por ejemplo autenticadores de hardware), deberá implementarse un procedimiento que incluya:

- Asignar la herramienta de autenticación.
- Registrar los poseedores de autenticadores.
- Rescatar el autenticador al momento de la desvinculación del personal.
- Revocar el acceso del autenticador, en caso de compromiso de seguridad.

La identificación del usuario se hará a través del formulario (Ver 3.5.3.6) que le proporcionará el gestor de seguridad, y se autenticará, mediante la firma impresa de la persona que tendrá acceso al sistema o se acreditará con su cuenta de usuario. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.

Cualquier petición de servicio de un empleado de GNN7 TV o un tercero, no se concederá si no es mediante la aprobación de la política de acceso a la información.

La cuenta temporal es usada únicamente con propósitos legales y de ejecución de tareas, por olvido de la información de la cuenta personal.

- La cuenta temporal es únicamente acreditable, si se proporciona la información necesaria para su uso.
- Toda cuenta nula u olvidada, se eliminará de los sistemas, previa verificación o asignación de una nueva cuenta, al usuario propietario de la cuenta a eliminar.
- El par usuario/contraseña temporal, será eliminada del sistema como tal, por el gestor de seguridad, en el preciso momento en que sea habilitada una cuenta personal para el usuario que haya solicitado su uso.
- El sistema no aceptará contraseñas con una longitud menor a la expresada en la política de creación de contraseñas.
- Los usuarios darán un seguimiento estricto sobre las políticas de creación de contraseñas, acatando sus disposiciones en su totalidad.
- El sistema revocará toda contraseña con una longitud mayor a la expresada en la política de creación de contraseñas.
- El usuario se responsabiliza en crear una contraseña fuerte y difícil de adivinar.
- Se recomienda utilizar una frase coma base para la creación de la contraseña, tomando la letra inicial de cada palabra.

El método específico de autenticación para cada sistema deberá ser proporcional con el nivel de sensibilidad del sistema para tener acceso (es decir, mientras más sensibles sean los sistemas se deberá utilizar métodos de autenticación más fuerte). Varios métodos de autenticación (por ejemplo, uso de la contraseña) pueden ser necesarios para la sensibilidad de alta confidencialidad o de alto riesgo.

Procedimientos y directrices

- Los usuarios no tendrán el acceso a los recursos de información GNN7 TV sin identificarse y autenticarse en ellos.
- Desarrollar y seguir los procedimientos para la creación, eliminación, y modificación de las cuentas de usuario y credenciales de autenticación.

- Las cuentas de usuario deben cumplir con las siguientes directrices:
    - Permitir sólo un usuario por cada cuenta. Los identificadores de usuario no deben ser compartidos. (Nombre de usuario, IDs).
    - Nunca se debe activar/habilitar una cuenta de invitado. Eliminar todas las cuentas que se crea de forma predeterminada por el sistema, a menos que sea absolutamente necesario, aprobado por el administrador de los sistemas.
    - No utilizar cuentas fáciles de predecir, tales como: anónimo, invitado, admin, FTP, telnet, usuario, test, otros por defecto.
- Las cuentas que están presentes por defecto en la instalación inicial del sistema, se deberán eliminar o cambiar de nombre a menos que sea técnicamente requerida por el sistema, debiendo dar aviso para tomar el resguardo necesario.
- Para las labores específicas que requieran cuentas de acceso (ya sea para algún funcionario o contratista), se deberán desactivar inmediatamente después del término de su utilización.
- Las cuentas deben ser desactivadas inmediatamente después del término de una labor específica que sea ejecutada por un empleado o contratista.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas de forma individual o combinada:

- Algo que solamente el individuo conoce, por ejemplo una clave secreta de acceso, una clave criptográfica, un número de identificación personal, etc.
- Algo que la persona posee: por ejemplo una tarjeta magnética.
- Algo que identifique al individuo, por ejemplo huellas digitales o la voz.
- Algo que el individuo es capaz de hacer, por ejemplo los patrones de escritura.

Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoría o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.

Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso. Detección de actividades no autorizadas. Además de realizar auditorías o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.

Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.

Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarios de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

Se debe anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación y a su vez debe ser registrado cualquier gestión de cambio eliminación o suspensión del usuario. (Ver 3.5.3.6)

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta; corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red de GNN7 TV y que no estén previstas en las políticas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.5.3.6 Formulario de registro de identificadores de usuarios

Utilizando este formato se podrá registrar la gestión de indicadores de los usuarios de GNN7 TV.

FORMULARIO DE REGISTRO DE GESTION DE IDENTIFICADORES DE USUARIOS										
IDENTIFICADOR	NOMBRE	APELLIDO	DEPARTAMENTO	FECHA DE CREACION	FECHA DE MODIFICACION	FECHA DE ELIMINACION	FECHA DE SUSPENSION	TIPO DE ACCESO	SISTEMAS	OBSERVACIONES

Figura #3.54: Formulario de registro de identificadores de usuarios

Elaborado por: Autores

3.5.3.7 Auditoria - Uso de los recursos del sistema

Objetivo

El objetivo de este control es identificar, documentar, revisar e implementar procedimientos seguros sobre el uso general de los recursos del sistema de información e informáticos de la organización así como también el uso de programas de utilidad del sistema que pudieran ser capaces de eludir los controles del propio sistema y de las aplicaciones asegurando así procesos eficientes de auditoría y seguridad informática y del negocio.

Alcance

El alcance de este control es establecer procedimientos seguros de gestión y buenas prácticas que permitan proporcionar una solución para controlar y preservar el uso adecuado y la integridad de los recursos de los sistemas informáticos y de información de la organización como: computadores, redes, sistemas de información, programas y datos propiedad de la organización.

Auditoria

GNN7 TV no cuenta con procedimientos adecuados para la gestión del uso de los recursos de los sistemas informáticos y de información, en algunos casos no están definidos los tipos de usos específicos y registros generales sobre cambios o alteraciones a los sistemas informáticos para con esto conocer de manera inmediata cualquier responsable por daños, pérdida o mala gestión del uso de los recursos.

Recomendaciones

- Todos los usuarios de los sistemas informáticos y de información se deben regir a la “Política del uso de los recursos del sistema” teniendo en cuenta que la misma debe ser cumplida para asegurar la eficiencia de los procesos de acceso sobre los sistemas informáticos y de información.

- Definir mecanismo de registro del uso adecuado de los recursos de los sistemas informáticos y de información para así evitar accesos no autorizados a los mismos.

- La utilización de algún recurso del sistema de GNN7 TV debe ser revisado y constantemente monitoreado para así asegurar que los usuarios designados están haciendo el uso de los mismos y no personas no autorizadas.

3.5.3.8 Políticas del uso de los recursos del sistema

Las políticas detalladas a continuación deben ser acatadas por todo el personal de GNN7 TV, tomando en cuenta que el uso de los recursos de los sistemas de información e informáticos y sus procesos debe ser registrado, controlado y gestionado por el área de TI de la organización.

El acceso y uso a los recursos del sistema de determinados servicios y aplicaciones ofrecidas por GNN7 TV requiere ser registrada a través de un mecanismo de reportes, sobre los incidentes relacionados al uso incorrecta de los recursos del sistema; estos pueden ir desde cambios en los servicios informáticos de la organización hasta manipulación de información. El área de TI debe establecer rutinas de auditoría de revisión del uso de los recursos del sistema de la organización para que así se mantenga vigilada la integridad y confiabilidad de los sistemas de información y que la información que maneja no sufra cambios provocados por accesos no autorizados a los mismos.

Se considera uso adecuado de los recursos del sistema a lo siguiente:

- El almacenamiento de la información requerida para el desarrollo de las actividades laborales en los equipos y sistemas de información que son suministrados por el área de TI para este fin, evitando tener dicha información en otros equipos o dispositivos.

- Solo se debe tener información o sistemas de información cuando se tenga la certeza de que no se está violando los derechos de propiedad, lo que implica evitar utilizar, recibir, mantener o copiar información o sistemas de información, que estén protegidos por leyes de derechos de autor, así como la distribución y/o instalación de software “pirata” u otros productos que no estén licenciados, incluidos fotografías de revistas, libros, música u otras fuentes.
- Evitar tanto en su equipo de cómputo como en las que estén a su alcance que se almacene material con contenido pornográfico u ofensivo en los equipos asignados.

Apoyarse para la instalación de software en los lineamientos de “no a la piratería”, evitando utilizar software diferente al establecido por el área de TI para el desarrollo de las actividades. En caso de requerir software adicional deberá hacer la solicitud por escrito al área de TI. La responsabilidad sobre el software no autorizado en los equipos asignados es de la persona sobre la cual recae la asignación del equipo.

No introducir intencionalmente programas “maliciosos” o virus dentro de la red de datos y comunicaciones, ni acceder o forzar accesos a información sobre la cual no se tengan los permisos y autorizaciones adecuadas. El escaneo de puertos o el análisis de tráfico y vulnerabilidades de la red con el propósito de evaluar vulnerabilidades de seguridad, sólo se considera adecuado cuando se lleve a cabo por parte de los encargados de la seguridad de la información de GNN7 TV, u otras personas con una autorización previa.

Evitar realizar ataques para aprovechar vulnerabilidades identificadas en los servicios brindados por el área de TI o sobre la infraestructura de servicios de GNN7 TV con la finalidad de interrumpir, interferir, deshabilitar y en general cualquier aspecto que afecte la prestación de los servicios o para propósitos que vayan en contra las personas, instituciones o deriven en incumplimiento de las leyes nacionales e internacionales.

Evitar que se ejecute cualquier forma de monitoreo de red, con la finalidad de interceptar datos que viajan por las redes de comunicación de GNN7 TV. Evitar que se adicionen equipos de cómputo o dispositivos a la red de datos que no hayan sido autorizados por el área de TI. Evitar participar en la difusión de información sin la debida autorización de los usuarios y los propietarios y custodios de la información; no enviar mensajes de correo no solicitados, incluyendo "junk mail" (material publicitario enviado por correo) o cualquier otro tipo de anuncio comercial a personas que nunca han solicitado dicho material (correo spam, correos electrónicos masivos, no solicitados o no autorizados). No generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola. Evitar la utilización de los elementos informáticos de GNN7 TV para hostigar o acosar a cualquier persona o compañía.

La utilización de los privilegios en los sistemas de información debe ser realizada para el cumplimiento de su labor y evitar el obtener información de usuarios que pueda considerarse violatoria de los derechos de intimidad, así como evitar realizar cambios no autorizados, e ir en contra de las funcionalidades para los cuales los sistemas de información están definidos que impacten la confidencialidad, integridad y disponibilidad de la información y los medios de procesamiento.

GNN7 TV brindará los aspectos para que los recursos de ancho de banda sean los adecuados para la prestación de los servicios y por esta razón velará porque estos aspectos se encuentren disponibles. En caso de ser necesario la utilización específica de estos servicios (videoconferencias, streaming de video, entre otros) para apoyar las actividades misionales se podrá habilitar el uso en horarios fuera del laboral con el fin de impactar de manera baja a los usuarios de la organización; salvo casos explícitos; para el uso de estas posibilidades se deberá hacer la solicitud por escrito previamente para realizar las autorizaciones respectivas en los elementos de control de ancho de banda que administra el área de TI. El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido al usuario administrador. Los administradores de servicios, tendrán acceso único a los módulos de configuración de las respectivas aplicaciones que tienen bajo su responsabilidad.

Todo servicio provisto o instalado en los servidores, correrá o será ejecutado bajo cuentas restrictivas, en ningún momento se obviaran situaciones de servicios corriendo con cuentas administrativas, estos privilegios tendrán que ser eliminados o configurados correctamente. Se registrará y archivará toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de "Log" o bitácoras de sistemas (Ver 3.5.3.9).

Los archivos de registro, almacenarán nombres de usuarios, nivel de privilegios, IP de terminal, fecha y hora de acceso o utilización, actividad desarrollada, aplicación implicada en el proceso, intentos de conexión fallidos o acertados, archivos a los que se tuvo acceso, entre otros.

Mantenimiento

El mantenimiento de las aplicaciones y software de sistemas es de exclusiva responsabilidad del personal de la unidad de informática, o del personal de soporte técnico. El cambio de archivos de sistema, no es permitido, sin una justificación aceptable y verificable por el gestor de seguridad. Se llevará un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación (Ver 3.5.3.10)

Uso de utilitarios de sistema

La mayoría de las instalaciones informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

- Utilizar procedimientos de autenticación para utilitarios del sistema.
- Separar entre utilitarios del sistema y software de aplicaciones.

- Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
- Evitar que personas ajenas al organismo tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.
- Establecer autorizaciones para uso ad hoc de utilitarios de sistema.
- Limitar la disponibilidad de utilitarios de sistema, por ejemplo durante el transcurso de un cambio autorizado.
- Registrar todo uso de utilitarios del sistema.
- Definir y documentar los niveles de autorización para utilitarios del sistema.
- Remover todo el software basado en utilitarios y software de sistema innecesarios.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta; corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red de GNN7 TV y que no estén previstas en las políticas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.5.3.9 Formulario de registro de incidentes de recursos del sistema

Utilizando este formato se podrán registrar los incidentes en cada recurso informático de GNN7 TV.

FORMULARIO DE REGISTRO DE INCIDENTES DE LOS RECURSOS INFORMATICOS							
FECHA	AREA	SUCURSAL	NOMBRE DEL RECURSO	OPERADOR/TECNICO	INCIDENTE	SOLUCION	OBSERVACIONES

Figura #3.55: Formulario de registro de incidentes de recursos del sistema

Elaborado por: Autores

3.5.3.10 Formulario de registro de mantenimiento de recursos del sistema

Utilizando este formato se podrán registrar los mantenimientos dados a los recursos informáticos de GNN7 TV.

REGISTRO DE MANTENIMIENTO DE LOS RECURSOS INFORMATICOS						
FECHA	AREA	SUCURSAL	TIPO DE RECURSO	OPERADOR/TECNICO	MOTIVO	OBSERVACIONES

Figura #3.56: Formulario de registro de mantenimiento de recursos del sistema

Elaborado por: Autores

3.5.3.11 Auditoria - Desconexión automática de sesión

Objetivo

El objetivo de este control es identificar, documentar, revisar e implementar procedimientos seguros sobre el uso general de los recursos del sistema de información e informáticos de la organización así como también el uso de programas de utilidad del sistema que pudieran ser capaces de eludir los controles del propio sistema y de las aplicaciones asegurando así procesos eficientes de auditoría y seguridad informática y del negocio.

Alcance

El alcance de este control es establecer procedimientos seguros de gestión y buenas prácticas que permitan proporcionar una solución para controlar y preservar el uso adecuado y la integridad de los recursos de los sistemas informáticos y de información de la organización como computadores, redes, sistemas de información, programas y datos propiedad de la organización. Se deberían desconectar las sesiones tras un determinado periodo de inactividad.

Auditoria

GNN7 TV no cuenta con procedimientos adecuados para la gestión de la desconexión automática de sesión de los sistemas informáticos y de información, en algunos casos no están definidos los tipos de conexión o desconexión automática de sesiones sobre cambios o alteraciones a los sistemas informáticos y así con esto conocer de manera inmediata cualquier responsable por daños, perdida o mala gestión del uso de los recursos.

Recomendaciones

- Todos los usuarios de los sistemas informáticos y sistemas de información se deben regir a la “Políticas de desconexión automática de sesión” teniendo en cuenta que la misma debe ser cumplida estrictamente para asegurar la eficiencia de los procesos de acceso sobre los sistemas informáticos y de información.
- Definir mecanismo de registro de la desconexión automática de sesiones creadas en los sistemas informáticos y de información para así evitar accesos no autorizados a los mismos.
- Definir tipos y perfiles de conexión para los diferentes usuarios de GNN7 TV tomando en cuenta diferentes factores como los horarios de trabajo, acceso a los sistemas, los tipo de trabajo a realizar y conexiones que realizan diariamente.

3.5.3.12 Políticas de desconexión automática de sesión

Las políticas detalladas a continuación deben ser acatadas por todo el personal de GNN7 TV, tomando en cuenta el proceso de desconexión automática de sesión en los sistemas de información e informáticos deben ser registrados, controlados y gestionados por el área de TI de la organización.

La desconexión automática de la sesión dentro de los sistemas de información ofrecidas por GNN7 TV requiere ser registrada a través de un mecanismo de reportes, sobre los incidentes relacionados al uso incorrecta de los recursos del sistema; estos pueden ir desde cambios en los servicios informáticos de la organización hasta manipulación de información. El área TI debe establecer rutinas de auditoría de revisión de las conexiones automáticas de sesión de los usuarios a los sistemas informáticos de la organización para que así se mantenga vigilada la integridad y confiabilidad y que la información que maneja no sufra cambios provocados por accesos no autorizados a los mismos.

El responsable de seguridad informática junto con los propietarios de la información definirá cuáles son los sistemas y conexiones consideradas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad, tiempo muerto, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla del terminal y deberá cerrar tanto la sesión de la aplicación como la de red. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal. Para las PCs, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si un agente debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

Limitación del tiempo de conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del periodo durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado. Se implementará un control y registro de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo áreas públicas o externas que estén fuera del alcance del SGSI de GNN7 TV (Ver 3.5.2.13). Entre los controles que se deben aplicar, se enuncian:

- Utilizar lapsos predeterminados, por ejemplo para transmisiones de archivos en lote, o sesiones interactivas periódicas de corta duración.
- Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.
- Documentar debidamente los agentes que no tienen restricciones horarias y las razones de su autorización, también cuando el propietario de la información autorice excepciones para una extensión horaria ocasional.
- Desconexión automática de terminales tras un periodo de inactividad establecido, especialmente los situados en lugares de riesgo, áreas públicas o no cubiertas por la seguridad de la organización, evitando el acceso a usuarios no autorizados.
- Limitación del tiempo de conexión a aplicaciones críticas, reduciendo la ventana de riesgo para accesos no deseados.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta;

corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red de GNN7 TV y que no estén previstas en las políticas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

3.5.3.13 Formulario de registro de conexiones automáticas de sesión

Utilizando este formato se podrán registrar los incidentes en los recursos informáticos:

FORMULARIO DE REGISTRO DE INCIDENTES DE LOS RECURSOS INFORMATICOS							
FECHA	HORA	AREA	USUARIO	JEFE DE AREA	SUCURSAL	SISTEMA	OBSERVACIONES

Figura #3.57: Formulario de registro de conexiones automáticas de sesión

Elaborado por: Autores

3.5.4 Objetivo de Control - Control de acceso a las aplicaciones e información

OBJETIVO: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación. Se debieran utilizar medios de seguridad para restringir el acceso a y dentro de los sistemas de aplicación. El acceso lógico al software de la aplicación y la información se debiera limitar a los usuarios autorizados.

3.5.4.1 Auditoria - Restricción del acceso a la información

Objetivo

El objetivo de este control es identificar, documentar, revisar e implementar procedimientos seguros sobre la restricción del acceso a la información de los sistemas de información e informáticos de la organización asegurando así procesos eficientes de auditoría y seguridad informática y del negocio.

Alcance

El alcance de este control es establecer procedimientos seguros de gestión y buenas prácticas que permitan proporcionar una solución para controlar, preservar y restringir el acceso a la información confidencial o no de los sistemas informáticos y de información que pertenecen a GNN7 TV.

Auditoria

GNN7 TV no cuenta con procedimientos adecuados para la gestión de restricción del acceso a la información de los sistemas informáticos y de información, en algunos casos no están definidos los tipos de accesos específicos y registros generales sobre cambios o alteraciones en los accesos a los sistemas informáticos y así con esto conocer de manera inmediata cualquier responsable por daños, pérdida o mala gestión del uso de los recursos.

Recomendaciones

- Todos los usuarios de los sistemas informáticos y de información se deben regir a la "Política del restricción de acceso a la información" teniendo en cuenta que la misma debe ser cumplida para asegurar la eficiencia de los procesos de acceso sobre los sistemas informáticos y de información.
- Definir mecanismo de registro de las restricciones a la información de los sistemas informáticos y de información para así evitar accesos no autorizados a los mismos.
- Monitorear constantemente que las restricciones de acceso a la información se esté cumpliendo por todo el personal de GNN7 TV y con esto asegurar que solo los usuarios designados están haciendo el uso de los mismos y no personas no autorizadas.
- Se deberían utilizar dispositivos de seguridad con objeto de restringir el acceso a las aplicaciones y sus contenidos.

- Se debería restringir el acceso lógico a las aplicaciones software y su información únicamente a usuarios autorizados.
- Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.
- Controlar el acceso de los usuarios a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.
- Proporcionar protección contra accesos no autorizados derivados del uso de cualquier utilidad, software del sistema operativo y software malicioso que puedan traspasar o eludir los controles del sistema o de las aplicaciones.
- No comprometer otros sistemas con los que se compartan recursos de información.
- Es importante dar acceso a la información y a los servicios únicamente a los usuarios que necesiten de esta para sus labores diarias.

3.5.4.2 Políticas de restricción de acceso a la información

Las políticas detalladas a continuación deben ser acatadas por todo el personal de GNN7 TV, tomando en cuenta el proceso de restricción de acceso a los sistemas de información e informáticos deben ser registrados, controlados y gestionados por el área de TI de la organización.

La restricción de acceso de los sistemas de información ofrecidas por GNN7 TV requiere ser registrada a través de un mecanismo de reportes, sobre los incidentes relacionados al uso incorrecta de los accesos al sistema. El área de TI debe establecer rutinas de auditoría de revisión de las restricciones de acceso a la información de los usuarios a los sistemas informáticos de la organización para que así se mantenga vigilada la integridad y confiabilidad y que la información que maneja no sufra cambios provocados por accesos no autorizados a los mismos.

El responsable de seguridad informática y los propietarios de la información deben definir cuáles son las restricciones de acceso a la información. Las mismas se harán efectivas para todo el personal de GNN7 TV sin excepción alguna.

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la política de control de acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la política para el acceso a la información. Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

- Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El propietario de la información involucrado será responsable de la adjudicación de accesos a las funciones, en el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, las mismas serán llevadas a cabo por personal del área de sistemas, conforme a una autorización formal emitida por el propietario de la información.
- Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.
- Controlar los derechos de acceso de usuarios (lectura, escritura y ejecución).
- Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.
- Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.
- Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

- Se acepta que los usuarios aprovechen en forma limitada los elementos informáticos para un uso personal que derive en su mejor capacitación, jerarquización y/o especialización en sus conocimientos, prácticas y habilidades o para aprovechar los beneficios de la informática.
- El uso aceptable no podrá interferir con las actividades o funciones que el usuario cumple, ni con la misión y gestión oficial del organismo o dependencia.
- Este uso personal podrá hacerse siempre que el recurso se encuentre disponible y no exista otro usuario que precise emplear el recurso para sus tareas laborales.
- El uso aceptado no se considera un derecho del usuario y se encuentra sujeto al estricto control permanente de la autoridad de aplicación y de la autoridad del organismo donde el usuario desempeña sus funciones.
- El uso aceptado puede ser controlado, revocado o limitado en cualquier momento por razón de la función, por cuestiones operativas y/o de seguridad de la red ya sea por la autoridad de aplicación y/o por los funcionarios responsables del organismo.
- No se considera uso aceptable aquel que demande un gasto adicional para el organismo, excepto el que derive del uso normal de los recursos informáticos.
- Bajo ninguna circunstancia el uso de los recursos informáticos por parte de los usuarios deberá influir de manera negativa en el desempeño, la imagen, en las tareas o generar responsabilidades para la organización.

Se definen expresamente como usos indebidos los siguientes:

- Modificar o reubicar equipos de computación, software, información, periféricos y/o cualquier otro medio de soporte de información (discos compactos, disquetes, cintas, etc.) sin la debida autorización del área de TI.
- Realizar cualquier actividad de recreación personal o de promoción de intereses personales (tales como creencias religiosas, hobbies, etc.).

- Modificar, alterar y/o borrar, sin las autorizaciones correspondientes, la información o las configuraciones de sistemas operativos o los aplicativos instalados por las personas autorizadas para tal efecto.
- Transgredir o eludir las verificaciones de identidad u otros sistemas de seguridad.
- Instalar o conectar cualquier equipamiento no autorizado.
- Acceder al código fuente de una obra de software sin autorización explícita del autor (área de software y aplicaciones) con la finalidad de modificarlo.
- Alterar, falsificar o de alguna otra forma usar de manera fraudulenta los archivos, permisos, documentos de identificación, u otros documentos o propiedades.
- Leer información o archivos de otros usuarios sin su permiso.
- Intentar obtener otros accesos distintos a aquellos que les hayan sido asignados.
- Difundir indebidamente y/o indiscriminadamente la información privada a que tuviere acceso con motivo de la función y actividad que desempeña.
- Intentar acceder a áreas restringidas de los sistemas de información.
- Intentar distorsionar o falsear los registros de los sistemas de información.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos.
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, o dañar o alterar los recursos informáticos.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable del organismo.
- Todo el personal que accede a los sistemas de información de GNN7 TV debe utilizar únicamente las versiones de software facilitadas por personal autorizado del área competente y siguiendo sus normas de utilización.

- La sustracción de equipos o periféricos informáticos, y/o cualquier otro medio de soporte de información (discos compactos, disquetes, cintas, etc.) constituyen un delito de acción pública.
- Se encuentra expresamente prohibido el uso de la red o de cualquier recurso informático que infrinja normas generales, causen daño o perjudiquen a GNN7 TV o terceros.

Se encuentra especialmente prohibido el uso de cualquier recurso informático para:

- Grabar, modificar o borrar software, información, bases de datos o registros del Poder Judicial, que no estén incluidas como tareas propias del usuario.
- Inferir cualquier daño a los equipos o a la información, las configuraciones de sistemas operativos o los aplicativos que se encuentren en ellos instalados.
- Acceder sin autorización a los sistemas de información de otros organismos.
- Obtener cualquier tipo de ganancia económica personal.
- Revelar o compartir contraseñas de acceso, propias o de terceros, con otros usuarios así como el uso de la identificación, identidad, firma electrónica o digital de otro usuario.
- Enviar cualquier transmisión de datos en forma fraudulenta.
- Introducir en los sistemas de información o la red contenidos obscenos, amenazadores, inmorales u ofensivos.
- Utilizar cualquier sistema de correo o cualquier tipo de comunicación electrónica con el propósito de revelar información privada de otras personas, sin su consentimiento.
- Utilizar cualquier sistema de correo electrónico o medio de comunicación electrónica con el propósito de dañar o perjudicar de alguna manera los recursos informáticos.

- Lanzar cualquier tipo de virus, gusano, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres cuya intención sea hostil, destructiva, o que afecte directamente en el funcionamiento adecuado de los diferentes sistemas y recursos informáticos.

- Realizar cualquier actividad contraria a los intereses de GNN7 TV, tal como publicar información reservada, acceder sin autorización a recursos o impedir el acceso a otros usuarios mediante el mal uso deliberado de recursos comunes.

- Alterar, falsificar o de alguna otra forma usar de manera fraudulenta los archivos, permisos, documentos de identificación u otros documentos o propiedades.

- Acceder, descargar, transmitir, distribuir o almacenar videos, música, imágenes, documentos y/o cualquier otro software o archivo cuya finalidad no se ajuste a la responsabilidad laboral de las funciones conferidas al agente.

- Violar cualquier ley o norma provincial o nacional, respecto al uso de los sistemas de información así como también realizar cualquier conducta ilegal contraria a la legislación aplicable de cualquier país al que se pueda tener acceso por la red.

Los usuarios de la red deben tomar los recaudos y la precaución para mantener su cuenta segura, es decir que no deben revelar bajo ningún concepto su contraseña o identificación a otro, a excepción en casos que deban facilitarse para la reparación o mantenimiento de algún sistema o equipo. En este caso y en forma estrictamente circunstancial, sólo deberá hacerlo al personal técnico o informático debidamente identificado, con la posibilidad que posteriormente dicho agente solicite al área técnica responsable, la modificación de claves, contraseñas u otro tipo de elemento de seguridad que implique riesgo de acceso por un tercero a los diferentes sistemas de información. Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña y contactar con el área de asistencia y capacitación técnica a usuarios para notificar la incidencia. Es responsabilidad del usuario el cuidado y buen trato de los recursos informáticos asignados.

Acción disciplinaria

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la gerencia. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del cargo dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta; corresponderá al departamento de recursos humanos hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de GNN7 TV. Todas las acciones en las que se comprometa la seguridad de la red de GNN7 TV y que no estén previstas en las políticas, deberán ser revisadas por la gerencia y recursos humanos para dictar una resolución sujetándose al estado de derecho.

CONCLUSIONES

El proyecto de grado presentado en este documento nos ha brindado la oportunidad de crear un esquema de procesos y buenas prácticas de seguridad informática y de información basada en la norma ISO 27002:2005, profundizando con esto el aprendizaje de procesos seguros en el tratamiento de la información.

GNN7 TV ha ido implementando algunos de los controles propuestos en este documento llevándolo así a corregir muchos de sus procesos actuales y de esta manera implementar no solo controles sino también indicadores de cumplimiento de los mismos.

El proyecto consta en su parte estructural no solo de recomendaciones en base a una auditoria sobre cada objetivo de la norma ISO 27002:2005 sino también en el estudio y soluciones de las mismas, facilitando así la toma de decisiones, documentación y registro de eventos sobre cualquier incidente informático y de información suscitado en la organización.

Se diseñaron formatos de control, actas y políticas a seguir para cada punto tratado en este proyecto de grado, brindándonos así facilidad de registro eventual, pasos a seguir para mejorar calidad de soporte brindado por el área de TI y sobre todo seguir un esquema de seguridad de procesos relacionados a la organización.

RECOMENDACIONES

Se recomienda automatizar en su totalidad los procesos de toma de inventario de activos informáticos mediante un sistema que permita almacenar y procesar toda la información de los mismos y que a su vez con la gestión adecuada logre llevar un mejor control de la propiedad de los activos, implementar jornadas de capacitación constantes para mantener al tanto a los usuarios sobre las políticas y responsabilidades que tienen sobre todos los recursos tecnológicos de la empresa.

Definir mejoras en los mecanismos de respaldo de GNN7 TV como el SAI, tomando en cuenta la necesidad actual y proyectando un crecimiento a corto y mediano plazo de todos los servicios informáticos a nivel de hardware y software de la empresa y a la vez planificar mantenimientos periódicos a todos los activos informáticos de propiedad de la empresa sin excepción. Implementar controles de seguridad para los activos que necesariamente deban salir de las instalaciones de GNN7 TV o deban ser dados de baja para evitar pérdida o fuga de información.

Implementar y gestionar la creación de esquemas organizacionales y asignar responsabilidades a los miembros del departamento de TI, registrando cada evento del SGSI en el que sean partícipes. Crear nuevos mecanismos de protección anti-malware para así contrarrestar el creciente riesgo de intrusión de código malicioso a los sistemas de información de GNN7 TV.

Reestructurar los roles por usuario y los permisos necesarios para cada uno de ellos mejorando así los mecanismos de acceso y autenticación a los sistemas de información de la empresa, a los recursos de red y a los sistemas operativos.

REFERENCIAS

Aglone3. (s.f.). Portal de Soluciones Técnicas y Organizativas a los Controles de ISO/IEC 27002. Obtenido de http://iso27002.es/

Aguilar R., Baker E, Gutiérrez C., y Liceaga C. (2009). Manual de Normas y Políticas de Seguridad Informáctica. Obtenido de http://www.tlalpan.uvmnet.edu/oiid/download/ISO%2027000_04_PO_ISC_PIT_E.pdf

Alvear e Yrigoyen. (2008). *Política de Seguridad de los Recursos Informáticos del Poder Judicial de Santiago del Estero.* Obtenido de http://www.jussantiago.gov.ar/jusnueva/Normativa/seguridad.php

Balestrini, R. (1997). *Técnica de la Investigación.* Mexico: Mc Graw Hill.

BSecure. (2010). *BSecure*.

Calder A., Watkins S. (2010). *Information Security Risk Management for ISO27001 / ISO27002.* Reino Unido: IT Governance Ltd.

Calder, A. (2006). *Information Security Based on ISO 27001/ISO 27002: A Management Guide.* Londres: Van Haren Publishing.

Cert, I. (2011). *Gestión de la Seguridad.* Obtenido de http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/demostrador/monografico_gestion_seguridad.pdf

Definicion.de. (2012). *Seguridad Informática*. Obtenido de http://definicion.de/seguridad-informatica/

Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman. (2000). *Building Internet Firewalls.* Estados Unidos: O'Reilly Media.

Garfinkel S., Spafford G. (2003). *Practical UNIX and Internet security.* Estados Unidos: O'Reilly Media.

Gemalto. (2010). *Data Loss Prevention*. Obtenido de http://www.gemalto.com/brochures/download/data_loss_prevention_esp.pdf

GNN7tv, J. d. (2013). *Organigrama de TI.* Guayaquil.

Gobierno de Chile. (s.f.). *Norma de uso Identificación y autentificación Ministerio del Interior*. Obtenido de http://www.intendenciaatacama.gov.cl/filesapp/Identificacion_y_autentificacion.pdf

Humphreys, E. (2007). *Implementing the ISO/IEC 27001 Information Security Management System Standard.* Norwood: Artech House.

Hunt, C. (2002). *TCP/IP Network Administration.* Estados Unidos: O'Reilly Media.

Intendencia Regional de Atacama. (2012). *Política y Procedimiento Preliminar de Control de Acceso.* Obtenido de http://www.intendenciaatacama.gov.cl/filesapp/Control%20de%20Acceso%20Preliminar.pdf

ISO. (2005). *ISO 27002 en Español*. Obtenido de http://iso27002.es/

ISO, N. (2005). *ISO 27001 en Español*. Obtenido de http://www.iso27000.es/sgsi.html

Marité, B. (12 de Diciembre de 2010). *Jefatura de Gabinete de Ministros de Argentina.* Obtenido de Gobierno de Argentina: http://www.jgm.gov.ar/archivos/pme/publicaciones/manual_gaf.pdf

Microsoft Corporation. (2013). *Administrador de Red.* Obtenido de http://technet.microsoft.com/es-es/library/cc626258(v=ws.10).aspx

Microsoft Corporation. (2013). *Antivirus.* Obtenido de http://www.micros oft.com/esxl/security/resources/antivirus-whatis.aspx

Miniwatts Marketing Group. (2012). *Exito Exportador*. Obtenido de http://www.exitoexportador.com/stats.htm

Oracle. (2011). *Guía de administración del sistema: servicios de seguridad.* Obtenido de http://docs.oracle.com/cd/E24842_01/html/E23286/concept-36.html

Osipav, V., Sweeney, M., & Weaver, W. (s.f.). *Cisco security specialist's guide to PIX firewalls.* Rockford, Mass: Syngress Pub.

Translinkqro. (Mayo de 2011). *Políticas De Uso De Los Recursos Informáticos En La Empresa.* Obtenido de http://www.buenastareas.com/ensayos/Politicas-De-Uso-De-Los-Recursos/2236342.html

Unidad de Gestión de Tecnologías de la Información. (julio de 2011). *Manual de Políticas Institucionales de Seguridad de la Información.* Obtenido de http://www.utpl.edu.ec/csirt-utpl/images/stories/manual.pdf

Universidad de Sevilla. (2011). *Presentación de Instancias y Solicitudes (Modelo Genérico) Guía Rápida del Procedimiento Telemático.* Obtenido de https://sede.us.es/c/document_library/get_file?uuid=73c9460a-ef6f-4706-bad4-a4aa4efe9315&groupId=10137

Universidad del Valle. (2010). *Políticas para el uso de recursos informáticos*. Obtenido de http://www.univalle.edu.co/politicainformatica/

Universidad Politécnica de Madrid. (s.f.). *Política de uso de los Recursos Informáticos y de la Red de Datos de la UPM.* Obtenido de http://www.upm.es/sfs/Rectorado/Vicerrectorado%20de%20Tecnologias%20de%20la%20Informacion%20y%20Servicios%20en%20Red/Servicio%20de%20Planificacion%20Informatica%20y%20Comunicaciones/Normativa/PoliticaUsoRecursosInformaticosRedDatos.pdf

Universidad de la República en Uruguay (2013). *Firewall y tipos de cortafuegos*. Obtenido de http://www.fing.edu.uy/tecnoinf/mvd/cursos/adminf/material/firewalls.pdf

Universidad Nacional Autónoma de México. (2010). *Auditoría en Informática.* Obtenido de http://fcasua.contad.unam.mx/apuntes/interiores/docs/98/8/audi_infor.pdf

WebQuest. (2010). *Vulnerabilidad y Riesgo*. Obtenida de http://webquest.carm.es/majwq/wq/ver/46330

ANEXOS

ANEXO #1: Acta de responsabilidad sobre los activos

ACTA RESPONSABILIDAD DE ACTIVOS	

Departamento:	
Jefe de Área:	
Custodio:	

FECHA	

Permanente (__) Temporal (__)

DESCRIPCIÓN DEL ACTIVO	CÓDIGO DEL ACTIVO

CLÁUSULA DE COMPROMISO
Como personal activo de GNN7 TV declaro que los activos indicados en el presente documento estarán bajo mi responsabilidad, por lo cual les daré un uso adecuado al desempeño de mis funciones y a la destinación institucional prevista para cada uno de ellos. En consecuencia serán asumidos por mi el daño o la pérdida de los mismos debidos a mi negligencia o incumplimiento de los instructivos relacionados con su uso y conservación. Me comprometo a informar y diligenciar el FORMATO UNICO PARA EL MOVIMIENTO de activos debidamente diligenciado y firmado por el Jefe o Coordinador de área, autorizando cualquier tipo de traslado requerido para dichos activos. Dado que la omisión de estas disposiciones es considerada como falta por el reglamento interno de trabajo, asumo las consecuencias económicas que conlleven a la pérdida de los bienes mencionados si ocurren por mi negligencia o incumplimiento de los instructivos correspondientes y en tal evento autorizo a la empresa XYZ a efectuar el descuento correspondiente al valor de reposición del bien afectado, deduciendo de mis salarios y prestaciones sociales o eventuales indeminizaciones a mi favor.

FIRMA CUSTODIO	FIRMA JEFE DE ÁREA	FIRMA JEFE DEL DEPARTAMENTO TI
_____	_____	
C.I:	**C.I:**	**C.I:**

ANEXO #2: Formato de salida y/o préstamo de activos fijos computacionales

Formulario de Salida y Prestamo de Activos Fijos Computacionales	
Fecha:	
Departamento Responsable:	
Nombre del Solicitante:	
Nombre del Jefe de Área:	
Código del Equipo:	
Fecha de Salida/Préstamo:	
Fecha de Devolución:	
Descripción del Equipo:	
Accesorios del Equipo:	
Código del Equipo:	

FIRMA DEL SOLICITANTE	FIRMA DEL JEFE DE ÁREA	FIRMA DEL JEFE TI
_____	_____	_____
C.I:	**C.I:**	**C.I:**

ANEXO #3: Formulario de solicitud de reubicación de los activos informáticos

Formulario de Solicitud de Reubicación de los Activos Informáticos	
Fecha:	
Nombre del solicitante:	
Departamento del Solicitante:	
Nombre del Jefe de Área:	
Localidad Actual del Equipo:	
Localidad a Reubicar del Equipo:	
Código de Inventario:	
Motivo de Reubicación:	
Observaciones:	

FIRMA DEL SOLICITANTE	FIRMA DEL JEFE DE ÁREA	FIRMA DEL JEFE TI
_____	_____	_____
C.I:	**C.I:**	**C.I:**

ANEXO #4: Formulario de registro de reubicación de activos informáticos

Formulario de Registro de Reubicación de Activos Informáticos	
Fecha:	
Nombre del solicitante:	
Departamento del Solicitante:	
Nombre del Custodio:	
Departamento del Custodio:	
Personal TI Responsable de	
Localidad Actual del Equipo:	
Localidad a Reubicar el Equipo:	
Código de Inventario:	
Descripción del Equipo:	
Motivo de Reubicación:	
Observaciones:	

FIRMA DEL SOLICITANTE	FIRMA DEL JEFE DE ÁREA	FIRMA DEL JEFE TI
_____	_____	_____
C.I:	**C.I:**	**C.I:**

ANEXO #5: Formulario de solicitud de mantenimiento de activos informáticos

Formulario de Solicitud de Mantenimiento de Activos Informáticos	
Fecha:	
Nombre del Custodio:	
Departamento:	
Jefe de Area:	
Código de Inventario:	
Equipo:	
Descripción del Problema:	

FIRMA DEL CUSTODIIO	FIRMA DEL JEFE DE ÁREA	FIRMA DEL JEFE TI
_____	_____	_____
C.I:	**C.I:**	**C.I:**

ANEXO #6: Acta de registro de mantenimiento de activos informáticos

Acta de Registro de Mantenimiento de Activos Informáticos	
Fecha:	
Nombre del Custodio:	
Departamento:	
Jefe de Área:	
Código de Inventario:	
Equipo:	
Marca / Modelo:	
No. de Serie:	
Fecha de Evaluación:	
Descripción del Problema:	
Diagnóstico:	
Propuesta de Reparación:	
Fecha de Reparación:	
Observaciones de Reparación:	

FIRMA DEL CUSTODIO	FIRMA DEL JEFE DE ÁREA	FIRMA DEL JEFE TI
_____	_____	_____
C.I:	**C.I:**	**C.I:**

ANEXO #7: Formulario de solicitud de salida de equipos de computación de la institución

Formulario de Solicitud de Salida de Equipos de Computación de la Institución	
Fecha de Salida:	
Fecha de Devolución:	
Nombre del Solicitante:	
Departamento:	
Jefe de Área:	
Equipo:	
Código de Inventario:	
Motivo de Salida del Equipo:	
Observaciones:	

FIRMA DEL SOLICITANTE	FIRMA DEL JEFE DE ÁREA	FIRMA DEL JEFE TI
_____	_____	_____
C.I:	C.I:	C.I:

ANEXO #8: Formulario de registro de activos fijos informáticos dados de baja

Formulario de Registro de Activos Fijos Informáticos dados de Baja	
Fecha:	
Nombre del Custodio:	
Departamento:	
Marca del Equipo:	
Modelo del Equipo:	
Número de Serie:	
Código de Inventario:	
Descripción del Equipo:	
Motivo para dar de baja al Equipo:	
Observaciones:	

FIRMA DEL CUSTODIO	FIRMA DEL JEFE DE ÁREA	FIRMA DEL JEFE TI
_____	_____	_____
C.I:	**C.I:**	**C.I:**

ANEXO #9: Formulario de solicitud de acceso a usuarios

Formulario deSolicitud de acceso a Correo Electrónico, Internet y a Aplicaciones de la Red			
PRIORIDAD:	ALTA	BAJA	INTERMEDIO

DATOS USUARIO (a rellenar en mayúsculas)			
Nombre (*):		Fecha:	
Apellidos (*):		Telf (*):	
Departamento(*):		Ciudad (*):	
Jefe de area (*):		Cargo (*):	

DETALLE GENERAL			
APLICACIÓN	PERFIL	MÁQUINA / BB.DD. (3)	OBSERVACIONES

SERVICIOS OFIMÁTICOS			
APLICACIÓN	PERFIL	MÁQUINA / BB.DD. (3)	OBSERVACIONES

CORREO ELECTRONICO:	SI	NO

OBSERVACIONES

Responsible	Autorizado por

(*) Dato obligatorio

El tratamiento de los datos de carácter personal que se realice para la "gestión de usuarios de sistemas de información",responsable del archivo y encargado de su tratamiento, se hará de conformidad con lo establecido a la Protección de Datos de Carácter Personal. Sobre dichos datos su titular podrá ejercitarlos derechos de acceso, rectificación, cancelación y oposición conforme a lo previsto en la normativa vigente.

ANEXO #10: Acta de petición de privilegios de usuario

ACTA DE PETICION DE PRIVILEGIOS
Por medio de la presente Yo, ……. , del departamento …… el …., ……., 20.. solicito se me concedan los siguientes accesos a los sistemas de información de la empresa GNN7 Tv, los cuales detallo a continuación:

SISTEMAS
1.
2.
3.
4.

Con el o los siguientes privilegios de usuario:

Adminsitrador		**Supervisor**		**Usuario**	

COMENTARIOS

La responsabilidad por el uso de los accesos a los sistemas solicitados es directamente responsabilidad del solicitante. Está prohibido su préstamo, de detectarse ingresos desde dos o más computadoras, el usuario responsable de la clave perderá inmediatamente sus privilegios de acceso y será además responsable por los contenidos visualizados en la o las demás computadoras y pasibles de las sanciones.

ANEXO #11: Acuerdo de confidencialidad de información

Guayaquil, ___ de _____ del 20___

Condiciones

Con el presente documento GNN7 TV y el Sr./Sra. _____ fijan formalmente y por escrito los términos y condiciones con el que ambas partes mantendrán la confidencialidad de la información propietaria de GNN7 TV. Para efectos de este acuerdo, tendrá la consideración de información confidencial, toda la información susceptible de ser revelada por escrito, de palabra o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro, intercambiada como consecuencia de este acuerdo. Este acuerdo no constituye ningún contrato, licencia o similar, obligando a las partes a adoptar las medidas oportunas para asegurar el tratamiento confidencial de dicha información y que no serán menores a las aplicadas por ambas a la propia información confidencial que manejan como parte de su labor.

Duración

Este acuerdo tendrá una duración indefinida desde el momento de su firma. _____ se compromete a mantener el compromiso de confidencialidad respecto a la información y material intercambiado entre las partes de forma indefinida tras la finalización del presente acuerdo.

Confidencialidad

El material entregado es confidencial y se compromete a:

- Utilizar dicha información de forma reservada.
- No divulgar ni comunicar la información técnica facilitada por GNN7 TV.

- Impedir la copia o revelación de información a terceros, salvo que gocen de aprobación escrita de GNN7 TV, y únicamente en términos de tal aprobación.
- Restringir el acceso a la información a sus empleados y subcontratados, en la medida en que razonablemente puedan necesitarla para el cumplimiento de sus tareas acordadas.
- No utilizar la información o fragmentos de ésta para fines distintos de la ejecución de este contrato.
- _____ será responsable, ante el incumplimiento de esta obligación, ya sea por sus empleados o por subcontratados.

Derechos previos sobre la información

Toda información puesta entregada a _____ es de propiedad exclusiva de GNN7 TV, _____ no utilizará información previa de la otra parte para su propio uso, salvo que se autorice lo contrario. La información que se proporciona no da derecho o licencia a GNN7 TV que la recibe sobre las marcas, derechos de autor o patentes que pertenezcan a quien la proporciona.

Derechos de propiedad

Toda información intercambiada es de propiedad exclusiva de la parte de la cual proceda. Ninguna de las partes utilizará información de la otra para su beneficio independiente.

Protección de datos

Para la correcta aplicación del presente acuerdo, _____ tendrá acceso a la información que es otorgada por _____

Confidencialidad del acuerdo

Las partes acuerdan que este documento tiene el carácter de confidencial y por tanto se prohíbe su divulgación a terceros.

Modificación o cancelación

Este acuerdo sólo podrá ser modificado con autorización expresa de ambas partes, en documento escrito y mencionando la voluntad de las partes de modificar el acuerdo.

_____

Firma del empleado

ANEXO #12: Acta de confidencialidad de las contraseñas

Datos personales

Nombre: _____ Apellidos: _____

Departamento: _____ C.I: _____

Jefe de Área: _____ Sucursal: _____

Manifiesta que el usuario tiene derecho y obligaciones a:

- Que dependido del desempeño de sus funciones, tiene acceso autorizado a datos de carácter personal e información confidencial de la organización.
- Que tiene conocimiento de la obligación de secreto profesional respecto de los datos de carácter personal y demás información confidencial a la que tenga acceso en el ejercicio de sus funciones, así como al deber de guardarlos y, en general al cumplimiento de las obligaciones y deberes relativos al tratamiento de datos personales, en virtud de lo dispuesto en cualquier normativa vigente, nacional y comunitaria, relativa a la protección de datos de carácter personal, y en particular a la legislación indicada en este documento.
- Que se compromete a cumplir las obligaciones mencionadas anteriormente, incluso después de culminada, por cualquier causa, su relación con GNN7 TV.
- Que se compromete a no revelar a persona alguna ajena o interna a la organización, sin su consentimiento, cualquier contraseña e información a la que haya tenido acceso en el desempeño de sus funciones o que pudiera haber obtenido por su condición de empleado de GNN7 TV.
- La irresponsabilidad personal del uso indebido de las contraseñas frente a GNN7 TV y frente a terceros puede causar daños y perjuicios que se pudieran ocasionar, derivados de un incumplimiento doloso de las obligaciones en

materia de protección de datos en las cuales GNN7 TV tiene el derecho de sancionar como consecuencia de dicho incumplimiento.

- Queda terminantemente prohibido dar las contraseñas de acceso a los sistemas de información a terceros u otros miembros de la organización; las contraseñas son de uso personal, intransferible e irrevocable para el acceso a los sistemas de información e informáticos de la organización.

_____

Firma del empleado

ANEXO #13: Formulario de identificación y autenticación de usuario

Nombres	**Apellidos**	**C.I.**
Departamento	**Jefe de área**	**Fecha**
Sistema(s)		
Correo Electrónico	**Identificador**	
Autenticación		
Comentarios		

Yo, _____ acepto las condiciones de creación de identificador y autenticación registrado mediante este documento.

_____

Firma del usuario

INDICE DE ABREVIATURAS

TI	Tecnologías de Información
SGSI	Sistema de Gestión de Seguridad de la Información
ISO	Organización Internacional para la Estandarización
IEC	Comisión Electrotécnica Internacional
ITU	Unión Internacional de Telecomunicaciones
CCITT	Comité Consultivo Internacional Telegráfico y Telefónico
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
ANSI	Instituto Nacional Estadounidense de Estándares
IEFT	Grupo de Trabajo de Ingeniería de Internet
FTP	Protocolo de Transferencia de Archivos
TCP	Protocolo de Control de Transmisión
UDP	Protocolo de Datagrama de Usuario
OSI	Modelo de Interconexión de Sistemas Abiertos
IP	Protocolo de Internet
MAC	Dirección Control de Acceso al Medio
URL	Localizador de Recursos Uniforme
HTTP	protocolo de transferencia de hipertexto
DLP	Prevención de Pérdida de Datos
SMTP	Protocolo para la Transferencia Simple de Correo Electrónico
IMAP	Protocolo de Acceso a Mensajes de Internet
POP3	Protocolo de Oficina Postal 3
VPN	Red Privada Virtual