***TABLA DE DISTRIBUCIÓN Y EMISIÓN DE DOCUMENTOS***

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Usuario** | **Fecha Entrega** | **Firma recibido** | **Digital** | **Físico** | **Copia No.** | **Difusión** | **Responsable Difusión** | **Fecha Difusión** |
| Alba Restrepo |  |  |  |  |  |  |  |  |
| Juan Diego Ramirez |  |  |  |  |  |  |  |  |
| Andrés Betancourt |  |  |  |  |  |  |  |  |
| William Cifuentes |  |  |  |  |  |  |  |  |
| Elkin Giraldo |  |  |  |  |  |  |  |  |
| Juan David Salazar |  |  |  |  |  |  |  |  |
| Esteban roldan |  |  |  |  |  |  |  |  |
| Edwin Ciro |  |  |  |  |  |  |  |  |
| Ana María Valencia |  |  |  |  |  |  |  |  |
| Felipe Restrepo |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**NOTA:**

Cuando se define que el documento debe tener una difusión, debe quedar la evidencia de la misma en el formato FPS01-Asistencia Capacitación y será responsabilidad de la persona asignada entregar el registro al sistema de gestión calidad.

Cuando se define que el documento NO requiere difusión a todo el equipo, queda bajo la responsabilidad del líder del proceso reforzar el correo con la actualización enviada desde el sistema de gestión.

|  |  |
| --- | --- |
| Revisó:  Asistente Sistemas | Aprobó:  Jefe de Sistemas |

\\10.1.2.67/Calidad/Aseguramiento/Procedimientos/IAQ16

MODIFICACIONES

|  |  |  |
| --- | --- | --- |
| **Fecha** | **Revisión** | **Descripción** |
| 01-08-2016 | 1 | Se realiza y difunde el procedimiento. |
|  |  |  |

|  |  |
| --- | --- |
| Revisó:  Asistente Sistemas | Aprobó:  Jefe de Sistemas |

**1. OBJETO**

El objeto de este procedimiento es establecer y documentar los procesos más sensibles para el área de sistemas en ALICO S.A para elaborar, revisar, aprobar, emitir, distribuir y actualizar los sistemas de información de la empresa.

**2. ALCANCE**

Con este procedimiento se busca dar una idea clara sobre los procesos realizados por el área de IT de la compañía, pasando por los procesos que tiene contacto a esta Área (administrativos y planta).

**3. DEFINICIONES**

* 1. **Backup’s:** paquete de datos realizado sobre un determinado sistema o archivos, el cual queda almacenado en un sitio especial digital como copia de seguridad.
  2. **Política:** es una secuencia de pasos que se debe cumplir para dar orden y realizar una acción dentro de la compañía.
  3. **Inspección**: proceso de corto tiempo que lleva a realizar una revisión verídica de un hecho o proceso.
  4. **Autorización:** persona o acción que lleva a realizar una acción sobre un proceso o hecho del área de IT con el aval de un cargo superior de la compañía.
  5. **Servidor:** es un equipo con altas capacidades en sus elementos, el cual le permite hospedar un conjunto de [aplicaciones](https://es.wikipedia.org/w/index.php?title=Computer_appliance&action=edit&redlink=1) que tiene gran demanda dentro de una [red](https://es.wikipedia.org/wiki/Red_de_computadoras)

**3.6 Rack**: un soporte metálico destinado a alojar equipos de tipo electrónico, informático y de comunicaciones.

**4. RESPONSABILIDADES**

**4.1 Jefe de Sistemas**

* Garantizar la realización oportuna de los backups.
* Realizar una inspección aleatoria sobre la realización de los backups de la compañía.
* Garantizar que la información esté disponible en cualquier momento requerido por personal de la compañía y que tenga la debida autorización.
* Suministrar los espacios adecuados para el almacenaje de información o Backups de la compañía.
* Planear y garantizar los mantenimientos preventivos de los equipos.

**4.2 Personal de Sistemas**

* Encargados de dar soporte sobre los sistemas de la compañía.
* Garantizar que la compañía este siempre en línea con todos los sistemas que posee.
* Interactuar con otras áreas para la solución de inconvenientes que afecte los sistemas de información de la compañía, redes, entre otros.
* Informar inmediatamente a su superior de daños relacionados con el área de sistemas.

**4.3 Director Infraestructura**

* Instalación de puntos de red en puestos de trabajo y máquinas.
* Instalación de los rack de datos.
* Planeación e instalación de nuevas áreas de trabajo.
* Mantenimiento de limpieza mensual de los rack de datos.
* Correctivos a los rack de datos y puntos de red en los puestos de trabajo.
* Instalación de los enlaces de rack en fibra óptica.

**4.3 Líderes de Epicor**

* Ayudar en el primer nivel de servicios sobre el sistema Epicor, para dar solución a un inconveniente de proceso, en caso de no poder dar solución, escalar al siguiente nivel de servicio que es el área de soporte de la compañía.
* Enviar a sistemas el formato de creación de usuario con los respectivos niveles de seguridad que el usuario tendrá dentro del sistema.

**4.4 Líderes de Proceso**

* Garantizar que las personas usuarias de los equipos tienen el conocimiento básico en manejo de herramientas ofimáticas, riesgos en el uso y buen manejo de la información.
* Garantizar que la información del proceso tiene las copias de seguridad para evitar pérdidas en la misma.

**4.5 Gestión Humana**

* Informar al área de sistemas los retiros de las personas de Alico.

**4.6 Usuarios**

* Responsables del buen uso de la información generada a través del sistema Epicor y generada en cada proceso.
* Reportar cualquier anomalía a su usuario líder si se trata de un problema en el ERP de la compañía.
* Reportar al proceso de sistemas problemas del hardware (computador, impresora), como mal funcionamiento, entre otros.
* Tener un buen uso de los equipos entregados y mantenerlos en un correcto funcionamiento, no generando algún tipo de daño que pueda atentar contra la integridad del mismo.

**5. GENERALIDADES**

**5.1 SOLICITUD DE EQUIPOS, SOFTWARE, CORREO, INTERNET, PERMISOS DE EPICOR, ETC POR PARTE DE LOS USUARIOS**.

* Los usuarios realizan la solicitud al líder del proceso, quien después de avalar la adquisición del equipo, informa mediante correo al jefe de sistemas quien gestiona la adquisición del software o hardware, además también se encargará de la creación de correos entre otros.
* Para los permisos de Epicor el líder funcional de Epicor (persona que participo en la configuración del ERP para Alico) debe enviar un correo solicitando la asignación del permiso bajo los grupos de seguridad que conoce y si no existe uno al cual lo relaciona, debe solicitar la creación de un grupo de seguridad, esta solicitud se hace con el formato FAQ03 Creación de usuario.
  1. **POLÍTICAS DE USO DE EQUIPOS POR PARTE DE LOS USUARIOS**

Con el fin de tener un buen uso de los equipos informáticos de la empresa y de la información contenida en ellos, el proceso de sistemas hace entrega de los equipos de computo y hace firmar un documento (formato FGC11 Entrega de equipos de computo) donde se describen las siguientes políticas:

* Mantener el equipo limpio y organizado, ello encierra (no comer ningún tipo de alimento sobre el Equipo, como frituras, harinas o bebidas, en especial azucaradas).
* Almacenar la información correspondiente e importante para la empresa, abstenerse de guardar información personal.
* El equipo será entregado con el software solicitado para ejercer las funciones del cargo, en caso de requerir otro diferente, este debe ser solicitado por su líder al área de sistemas. Recuerde que el tener en su equipo software piratas o no autorizados, puede implicar GRANDES MULTAS PARA LA COMPAÑÍA.
* Asegurar que la información y/o los registros importantes del proceso tengan copia de seguridad o Backup para evitar la pérdida de información.
* Tener las precauciones debidas para evitar que se infecte su equipo de virus como por ejemplo ingresar a páginas de internet que no sean seguras o abrir correos de dudosa procedencia.
* Se debe tener la buena costumbre de borrar o depurar la información que se tiene obsoleta (por vieja o porque ya no es aplicable), con el fin de tener una información actualizada y de ser eficientes con respecto al almacenaje de información (memoria de los equipos de cómputo).
* Reportar al área de sistemas el daño del equipo o inconvenientes presentados en el manejo del mismo.
* Reportar al área de mantenimiento de infraestructura, el daño de la UPS.
* En caso de retiro de la empresa, el equipo debe ser devuelto en buenas condiciones al área de sistemas y deberá hacer firmar **el paz y salvo** del jefe de Sistema en el formato F-GH-05 Paz y Salvo de Egreso.

**5.3 ENTREGA DE EQUIPOS EN CASO DE RETIRO**

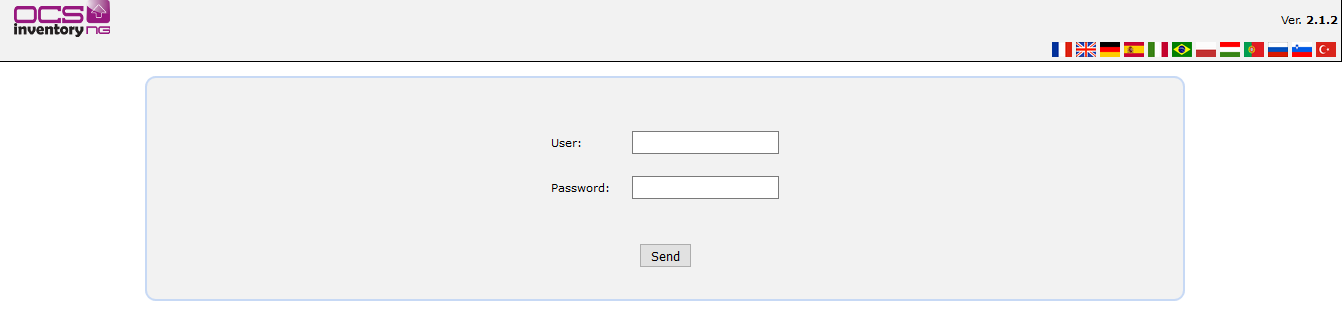
En el caso de que la persona se vaya a retirar de la empresa, se debe reportar al área de sistemas quienes deben firmar el paz y salvo de egreso F-GM-05 y sistemas debe:

* Eliminar el correo.
* Eliminar el usuario de Epicor (si aplica).
* Eliminar del computador la información personal.
* Definir junto con el proceso que se hace con el equipo, si se designa a otra persona o se retira del proceso. En caso de reasignación se debe volver a dar las políticas de uso de los equipos estipuladas por sistemas.

**5.4 INVENTARIO DE HARDWARE Y SOFTWARE**

**5.4.1 Hardware**

El área de sistema ha implementado un software Libre llamado OCS Inventory para llevar un registro del inventario de computadores, impresoras, software que posee instalados y de las características de cada computador que posee en este momento Alico, en el cual podemos saber, que versión de sistema operativo tiene, que office, que programa son pagos o licenciado o versión beta, libres o gratuitos, entre otros datos de utilidad para el área de IT. La forma de acceder a esta información es en la siguiente dirección en la red http://10.1.2.185/ocsreports/



Este archivo es alimentado cada que entra o se retira un equipo y también cada que se instala un programa ya sea por parte del usuario o del área de sistema, que corre un agente y lo notifica en la base de datos.

Con este software basado en la administración WEB, podemos determinar capacidades de los equipos y que adaptación de recursos es necesaria para estos, en un futuro cuando estos equipos presenten problemas en especial de desempeño.

**5.4.2 Software**

Alico, a través del OCS Inventory identifica la mayor parte del software que maneja cada computador como por ejemplo (Office, net framework, antivirus, navegadores, etc). En este punto se hace referencia a los softwares de mayor relevancia y que manejan la mayor información de Alico:

|  |  |
| --- | --- |
| Software | Usuario |
| Epicor | Sistema ERP de la empresa, donde se consolida toda la información de las diferentes áreas de la compañía, como producción, ingenierías, compras, ventas, movimientos financieros, mantenimiento, entre otros. |
| Angelnet | Software mediante el cual Alico realiza los registros de importación. |
| Isolucion | Software de gestión documental, administrado solo por el área de control y calidad. |
| Midasoft | Software utilizado por gestión humana para el manejo de nómina. |
| Adobe creative Cloud | Empleado para el proceso productivo de elaboración de diseño y desarrollo de preprensa. |
| Focuss | Enfocado a la planeación de los recursos |

Para términos de consulta de información, con fechas antes de Enero – 2015, se poseen las bases de datos del software Visual (ERP enfocado a costos) y Aplinsa (Enfocada a información financiera).

**5.5 MATRIZ DE RIESGOS.**

En Alico, tenemos la matriz de Riesgos corporativa donde se identifican los riesgos generales de empresa incluyendo los riesgos de pérdida de información. Esta matriz se encuentra ubicada en la ruta \\10.1.2.240\Indicadores\Indicadores 2017\Sistemas.

Alico, realizará una matriz enfocada al proceso de sistemas, donde se identifiquen las amenazas de los activos, las vulnerabilidades que podrían ser aprovechadas que impacten la confidencialidad, integridad y disponibilidad.

En esta matriz se realiza la valoración del impacto, la probabilidad de ocurrencia del riesgo, dando así un nivel de riesgo, el cual se determina su aceptación, tratamiento, evitar el riesgo o transferirlo.

Esta matriz aún no está desarrollada, es un propósito a futuro.

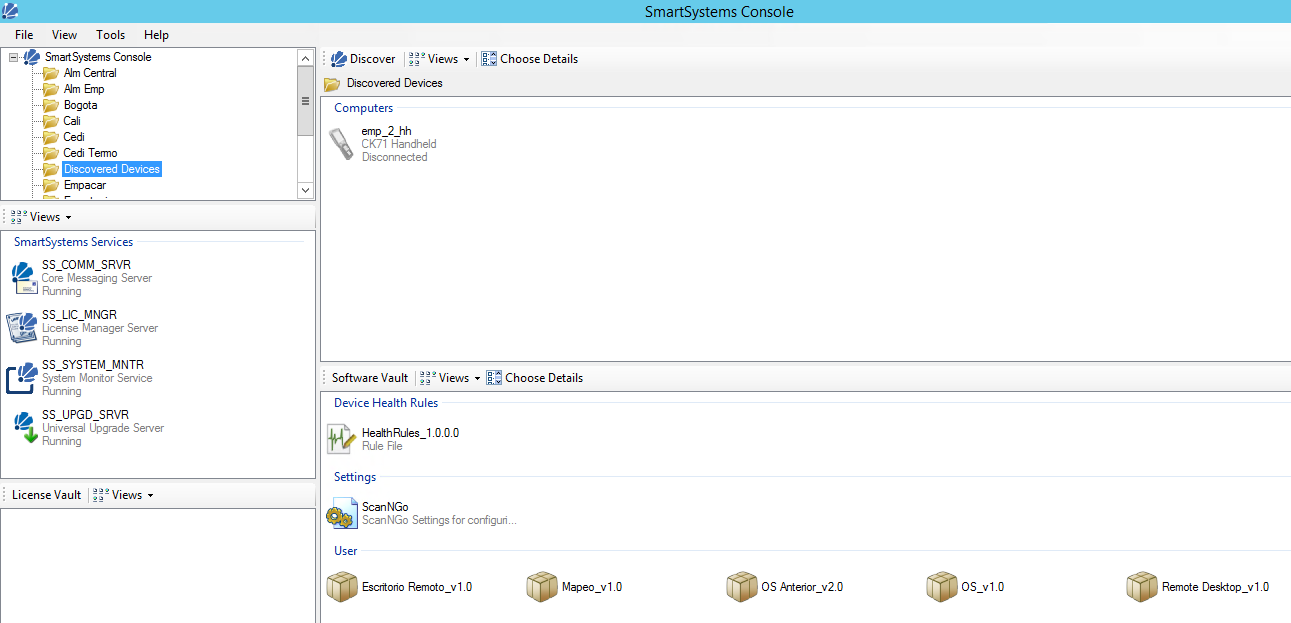
**5.6 MANTENIMIENTO DE LOS EQUIPOS**

El Área de sistemas tiene programado para los mantenimientos preventivos ciclos de cada 6 meses, aunque contantemente se está revisando Equipos y se hacen reparaciones Correctivas cada vez que un equipo presenta fallas.

Los mantenimientos son realizados por personal de sistemas, en caso tal, se evalúa la complejidad y se contrata un tercero para realizar la respectiva reparación.

Las Hand Held no tienen Mantenimiento preventivo, puesto que cuando el equipo presenta falla se realiza el correctivo y si el daño es severo, se llama al proveedor para que tome acciones sobre el equipo.

En muchos casos para dar soporte correctivo en la HH o asistencia al usuario, utilizamos un software gratis del proveedor, llamado Smartsystem, se anexa imagen



El reporte de mantenimiento preventivos y correctivos está alojado en uno de nuestros servidores locales en la siguiente URL.

\\10.1.2.240\Indicadores\Indicadores año (xxxx)\Sistemas\Indicadores Sistemas.xlsx

* 1. **SEGURIDAD DE LA INFORMACIÓN**

Con el fin de asegurar la información que se tiene en los diferentes procesos de la empresa, el área de sistemas se tienen algunos controles y herramientas preventivas, se listan a continuación:

* + 1. **BACK-UP DE LA INFORMACIÓN**

Según la criticidad de la información, se define la responsabilidad de la realización de las copias de seguridad de la siguiente manera:

1 -> Sistemas Alico

2 -> usuarios

3 -> Proveedor

|  |  |
| --- | --- |
| BACKUPS | VALOR |
| Servidor de Artes | 1 |
| Servidor de información 10.1.2.240 | 1 |
| Control Calidad (Algunos documentos) | 1 |
| Gerente Financiera | 1 |
| Directora Tesorería | 1 |
| Impuestos | 1 |
| Información de usuario | 2 |
| Epicor in site | 3 |
| Backup y Restauración de datos Epicor | 1 y 3 |
| Angelnet | 1 |
| Isolution | 3 |
| Midasoft | 1 |

**A continuación, se describe la forma y las frecuencias de las copias de seguridad.**

**5.6.1.1 Backup’s Servidor de Datos**

Alico posee un servidor de datos IP 10.1.2.240, donde los diferentes procesos de la empresa almacenan la información crítica, entre ella, se encuentran los indicadores y sus análisis, matrices de riesgo, matrices de requisitos legales, acciones correctivas y de mejora, etc. A este servidor todas las noches se le realiza una copia de seguridad, el cual, al presentarse algún suceso, los datos pueden restablecerse a la noche anterior del suceso.

**5.6.1.2** **Servidor de Artes**

Se realizan dos copias, una en un servidor alterno IP 10.100.1.49, esta copia se realiza los domingos, la otra copia se realiza en unos discos externos que quedan dentro del departamento de sistemas.

**5.6.1.3 Información de algunos computadores**

En el computador de Control-Calidad (IP 10.1.2.67), se le hace copia de seguridad los martes, jueves y viernes quedando la información en la NAS (IP 10.1.2.247).

Las Historias Clínicas del personal, se le hace copia de seguridad los martes y jueves, esta información queda almacenada en la NAS (IP 10.1.2.247).

Para los equipos de Gerencia Financiera (IP 10.1.2.43), Directora Tesorería (IP 10.1.2.56) e Impuestos (IP 10.1.2.78) se les realiza backups los martes y jueves en el mismo equipo y cada 8 días se les hace copia en la NAS (IP 10.1.2.92).

**5.6.1.4** **Información de usuarios críticos**

Alico realizo la compra de 100 licencias de office 365, el cual fue instalado a personal que maneja información importante de la compañía para que realizaran sus propios Backup’s en la nube, estas personas cuentan con un (1) Terabyte de almacenamiento por cada uno de ellos. Sistemas hizo entrega personalizada a los usuarios, los capacitó y se dejaron como responsables de realizar sus propios Backup’s.

**5.6.1.5** **Epicor**

La base de datos es administrada por el equipo IT de Alico, pero físicamente se encuentran en la ciudad de Bogotá, alojado en el data center de Claro y administrado por Ability, que ofrece el servicio de hosting, ellos con su equipo de IT también supervisan el funcionamiento de los servidores y velan porque siempre estén en servicio. Ellos son los que nos realizan Backup’s de nuestra información de la siguiente forma:

* **Lunes a Domingo:** se realizan dos Backup’s, uno se realiza al medio día, este Backup’s es almacenado en un servidor hasta la noche, cuando corre el siguiente Backup’s y hace borrado del que se realizó al medio día, este último Backup’s es descargado en el servidor de Replicación en Alico.
* **Semana a semana**: este Backup’s se realiza cada final de semana, es el Backup’s más completo de información que hay por semana sobre la compañía, es almacenado en Ability.
* **Final mes:** a final de mes, el sistema toma el último Backup’s realizado semana por semana y este es almacenado en un servidor de Backup’s que posee el proveedor Ability.

En Ability se guarda la última copia de la semana y así continuamente cada semana hasta completar un mes, es decir puede guardarse 4 o 5 Backup’s de semana y al llegar a este tope, guarda ya al final la última por cada mes y así durante un año.

El objetivo más preciso sobre los Backup’s diarios, es poder contar al día siguiente con una copia exacta de lo que hubo en el sistema hasta las 9 PM, desde Ability es trasmitido a través de un software a un servidor de pruebas que tenemos en Alico; Esta copia también sirve de contingencia por si se presenta algún problema de comunicación con Bogotá o nuestro ERP; se tiene para las áreas críticas y que pueda ejecutar sus funciones sin problema desde este servidor en Alico.

**Pruebas de restauración de copias o Backup’s:** todos los días al montar las copias en Alico, se puede detectar si existe un daño o problema en la copia descargada, en este caso, se coloca un “ticket” al proveedor para su análisis y se le solicita abrir el puerto para realizar nuevamente el descargue de la base de datos de la noche anterior en el servidor de Alico.

El Backup’s que se guarda en la noche en Alico es montado a primera hora en un servidor que tenemos de Replicación con el fin que, si se presentan un suceso en Bogotá, fácilmente las áreas más importantes, entre ellas despachos y logística puedan seguir operando al cabo de unos minutos en el sistema de replicación con la información que hubo a la noche anterior, para esto ya se estableció un procedimiento y los usuarios de esta área creados y listos para acceso en el servidor de replicación.

**5.6.1.6 Angelnet**

De esta informaciónse realiza Backup’s diarios en la noche, el área de IT es el encargado de dar soporte en este software a nivel Alico, en caso de tener problemas mayores, estos se escalan al proveedor.

**5.6.1.7** **Isolucion**

Software de gestión documental, administrado solo por el área de control y calidad, quienes podrán ingresar, modificar o eliminar información, mientras que los usuarios que accedan a el por medio de la Red solo tendrán permisos de visualización, el soporte a este software es dado por el tercero que lo ofreció.

**5.6.1.8 Midasoft**

Software para la gestión de nómina, administrado por el área de Analistas de nomina de la compañía, a este software se le realiza todas las noches copias de seguridad, que son almacenada en el servidor 10.1.2.6 y Diariamente también se le realiza una copia en la NAS IP 10.1.2.247

* + - 1. **Página web y la Intranet**
* La página web de Alico es administrada por un tercero, quien es el encargado de Administrar gran parte de ella como también velar que no sea vulnerable a ataques externos. La responsabilidad de este contrato es por parte del área de mercadeo en el proceso de Ventas. A esta página web se le hace copia de seguridad cada 2 meses y es responsabilidad del proveedor.
* La intranet, es administrada en conjunto por comunicaciones y sistemas. Se hace copias de seguridad todos los días y es almacenada este backup por ocho días. Con la entrada en vigor de Google apps esta intranet esta obsoleta y se construirá una nueva intranet en la aplicación Google site, esta tarea esta a cargo del área de Mercadeo y Comunicaciones de la compañía.
  + 1. **SEGURIDAD DE LOS DATOS DE LAS REDES.**

En Alico existe dos redes una que es en la que están todos los equipos y una para clientes:

* La red de los equipos de Alico, se divide en dos:
* La red LAN: Es una red cableada que es administrada por el equipo de Sistemas de Información y un tercero llamado Compuredes, donde a través de un DHCP este ofrece todo el direccionamiento IP para los equipos y son configurados por el área de sistemas.
* Red wifi Producción: En esta red están los equipos de planta, primero deben estar registrados con la dirección MAC en una controladora y además debe tener cierta configuración que brinda el equipo de Sistemas de Información para que el equipo sea reconocido en esta red.
* Red Wifi Invitados: es una red enfocada a los clientes y visitantes de Alico, esta red posee una clave que cada 8 días el personal IT cambia, con el fin de sacar equipos que no deban estar allí y que por algún motivo obtuvieron la clave, con ello se evita consumos innecesarios y ocupación de la red para otros fines.
  + - 1. **Administración de Redes**

Para mantener, controlar y proteger contra amenazas las redes y aplicaciones que usan la red se trabaja con un tercero, llamado Compuredes, con ellos se tiene la administración de las redes de la empresa. Ellos prestan las herramientas necesarias para determinar en qué áreas está fallando la comunicación, dónde existen consumos excesivos de datos, qué dispositivo está intermitente. Llevan estadísticas de consumos de red (horas pico, congestión de red, velocidades de los datos, perdidas de paquetes, entre otros). En caso de que Alico necesite de esta información se solicita al proveedor.

* + - 1. **Firewall (Pared de Fuego)**

Alico cuenta con un firewall que consiste en una barrera que nos protege de las mayores vulnerabilidades que existen en la red mundial. Este Firewall fue contratado con una de las grandes empresas en Colombia (ETB), quien es la encargada de administrar y velar por la seguridad perimetral de la empresa, como son ataques de Crackers. Además, este Firewall analiza el servicio de mensajería para prevenir posibles ataques mediante spam u otros elementos ya detectados por ellos, este firewall mediante políticas definidas por el departamento de sistema realiza filtro de contenido para la navegación web.

* + - 1. **Antivirus**

Alico para evitar la intrusión de códigos maliciosos, ya sea por medio de correos, memorias USB, discos externos, páginas Web, tiene instalado en los equipos de cómputo de la empresa el antivirus McAfee, que está entre el top 5 de las mejores empresas de antivirus. La actualización de estese realiza automáticamente cada vez que el mismo programa lo vea necesario y es transparente para el usuario final. Cabe anotar que los antivirus no detectan los nuevos virus liberados en la red.

* + 1. **SEGURIDAD EN LAS INSTALACIONES FÍSICAS**

Con el fin de prevenir un daño o pérdida de la información de Alico, se tiene un control en el ingreso a las áreas físicas donde se encuentran los servidores que manejan la información y los centros de cableado y rack de datos.

**5.6.3.1 Servidores**

En Alico, se tienen los servidores tanto de la información como los de los backup ubicados en la oficina de sistemas y en el rack principal ubicado al lado de Soporte técnico.

El acceso a estos servidores es restringido para personal de sistemas y de infraestructura.

* + - 1. **Seguridad de cableado de la red**

El cableado se encuentra instalado de acuerdo con estándares internacionales de redes de datos, se usa topología tipo estrella, donde existe un rack principal de donde se derivan hacia los racks secundarios ubicados en cada una de las áreas de la empresa.

La instalación del cableado y del centro de cableado se hace según las especificaciones de las normas internacionales (para más información remitirse al departamento de infraestructura) con el fin de evitar daños físicos por manipulación.

* + - 1. **Rack**

En Alico se tienen los siguientes centros de cableado y rack de datos:

|  |  |
| --- | --- |
| No. | Ubicación |
| 0 | Bodega 0 - Oficinas de Mantenimiento e Ingeniería |
| 1 | Bodega 1 – Oficina de Financiera |
| 2 | Bodega 2 – Oficinas de Fundas |
| 3 | Bodega 3 – Piso No. 2 |
| 4 | Bodega 4 – Piso No. 4 |
| 5 | Bodega 5 – Contiguo al laboratorio |
| 6 | Bodega 6 – Oficinas de Gestión Humana |
| 7 | Bodega 7 – Oficinas Termoformado |
| 8 | Bodega 8 – Oficinas Exportaciones |
| 9 | Bodega 9 – Oficinas Puerta sur y puerta norte |
| 10 | Bodega 10 – Ventas piso 2 y 3 |
| 11 | Bodega 11 – Oficina de Almacén central |

Estos racks se encuentran dentro de instalaciones encerradas y el ingreso es con llave, además el mueble del rack también tiene una puerta con llave.

* + 1. **CONTROLES PARA EVITAR PERDIDAS DE INFORMACIÓN DE LOS USUARIOS FINALES**
       1. **Buen Uso por parte de los usuarios**

Los usuarios deben garantizar el buen uso y el cuidado tanto de los equipos como de la información que ellos guardan, para esto deben de cumplir con las indicaciones dadas por el área técnica de informática y tener cuidado de no abrir correos de sospechosa procedencia o con extensiones no conocidas.

**5.6.4.2 Protección de los equipos contra fallas en el suministro de energía u otras anomalías.**

En Alico se poseen UPS que dan soporte a la hora de tener un fallo en el suministro de energía, la principal que está en el rack cuenta con una autonomía de 30 a 45 minutos, las Ups para los servidores que están en el área de IT tienen un tiempo estimado aproximadamente 10 min y cada equipo de los usuarios posee una Ups con un t*i*empo de 10 min.

Referente al ERP de la empresa, por estar en el bunker de Claro, ellos cuentan allá con su planta de energía para seguir dando servicio, aunque esta caída el sistema normal de energía.

* + - 1. **Control para evitar instalaciones de software**

El equipo de IT en todos los computadores se está instalando una cuenta administradora y una de usuario, en la cual la administradora permite al equipo de IT realizar los cambios necesarios.

La cuenta administrador es protegida bajo una contraseña y la otra cuenta es la de acceso de los empleados de la compañía, esta cuenta posee limitaciones de ejecución e instalación, desde allí pueden ejecutar sus programas para su labor.

Los Gerentes de la empresa no poseen estas restricciones, ya que son conocedores de las implicaciones legales que puede traer la instalación de un software que no es licenciado.

* + - 1. **Restricción a la salida de páginas en la internet**

Por medio de la herramienta Fortinet que se adquirió desde el 2016, se realizan restricciones y bloqueos a determinadas paginas web, limitando así el uso inadecuado de la red, en ciertos casos y autorizados por el jede del área se dan ciertos privilegios para dar mayor acceso a la navegación.

**5.6.4.5Seguridad de los equipos fuera de las instalaciones**.

En Alico se tienen varios portátiles para los cuales existe una póliza de Robo físicamente y cada usuario es responsable de su información.

5.6.4.6 **Hacking**

Dentro del contrato con el Proveedor ETB se tiene contemplado el monitoreo para ataques, los cuales, si se llegan a presentar, serán analizados con el jefe de sistemas, con el fin de ir mejorando la seguridad perimetral de la compañía. Anexo a esto se tiene la cotización de una empresa externa para realizar otro estudio de **“Ethical Hacking y Análisis de Vulnerabilidades”,** el cual está pendiente de ser avalado, este servirá para tener una mejor referencia de nuestra compañía ante posibles ataques en el país.

La contingencia en este caso debe ser por parte del proveedor ETB, el cual realizara controles de inmediato y tomara las soluciones limítrofes e ipso factas para cerrar la brecha que se está presentando y entregar un informe detallado al jefe de sistemas de Alico.

**5.7 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL RETIRO DE ACTIVOS.**

En caso de eliminar o retirar un equipo de cómputo de la empresa, el equipo debe ser entregado a sistemas para realizar:

* El formateo de la información y garantizar que el mismo quede sin ninguna información o software instalado competente a la compañía.
* Enviar un correo a contabilidad informándoles el retiro de dicho equipo.
* Eliminarlo del inventario de equipos de Alico.

**5.8 ACTUALIZACIÓN DE LA INFORMACIÓN**

Sistemas de Información evalúa las necesidades de Alico ya sean presentes o futuras, busca y propone cuales software o hardware son los más adecuados al tamaño de la compañía y lo expone a Gerencia General, quien es la que determina si es viable o no la adquisición de los elementos teniendo en cuenta los presupuestos que se realizan anualmente en la revisión estratégica.

**5.9 INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y SU ANÁLISIS.**

Desde el 2015 la empresa invirtió en las adquisiciones de servicios y equipos que ayudan con el control y prevención de ataques, posible pérdida información por agentes externos; estos proveedores continuamente mediante software especializado realizan monitoreos diarios y ante un suceso, informan inmediatamente al jefe de sistemas de Alico y la posible solución dada a dicho inconveniente.

**5.14 INDICADORES Y TOMA DE ACCIONES**

El área de sistemas de información maneja sus indicadores en la ruta: [\\10.1.2.240/indicadores/indicadores](file:///\\10.1.2.240/indicadores/indicadores) año (xxxx)/Sistemas, estos indicadores se realizan con el fin de llevar el control de los equipos e ir tomando acciones que le permitan mejorar continuamente, además estos indicadores permite llevar un control de los informe que realiza el departamento mediante solicitud de los usuarios de cada área.

**6. PROCEDIMIENTO**

**6.1 Procedimiento con los usuarios.**

Uso adecuado y confiable, cumpliendo el reglamento.

Entrega de reglamento de uso.

Entrega de hardware o software

Solicitar software o hardware.

Usuario

Area IT

Area IT

Usuario

SI

Entregar el computador?

Formatear el computador y guardar información importante de la empresa.

Borrar información con periodicidad.

Realizar copia de seguridad.

Usuario

Usuario

Area IT

Atención al usuario de necesidades.

Reportar daños de hardware o software

Area IT

Usuario

**6.2 Procedimiento Area IT.**

Inventario de software y hardware.

Realizar y analizar matriz de riesgos.

Planeación de mantenimientos.

Control y Seguridad de la información

* Back up
* Seguridad de las redes (antivirus, firewall).
* Seguridad de las instalaciones físicas (servidores, cableado, rack).
* Controles para evitar pérdida en la información.

Análisis de incidentes y de indicadores de gestión.

Toma de acciones para mejorar indicadores, la gestión del proceso y ser efectivos.

**7. ANEXOS**

N.A.