POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

SGSI-POL-001-Politica_5.0

Autor: Sergio Franco **Empresa :** Rallo Hermanos S.A.	**Validado por:** Comité de Seguridad **Empresa :** Rallo Hermanos S.A.	**Aprobado por:** Gerencia **Empresa :** Rallo Hermanos S.A.
Fecha: 14/10/2015	**Fecha: 14/10/2015**	**Fecha: 14/10/2015**

Descripción: POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Control de Versiones:

Versión	**Fecha**	**Autor**	**Descripción de los cambios**
1.1	**06/05/2009**	Sergio Franco	Versión inicial de documento
1.2	**28/07/2009**	Sergio Franco	Cambio en la definición del alcance que queda referenciada a otro documento para evitar inconsistencias. Se ha incluido un punto de referencias. Se ha ampliado el punto de principios y objetivos
2.0	**09/06/2010**	Sergio Franco	Se detallan más las bases sobre las que se sustenta la política. Se adapta al formato de la política de calidad.
3.0	**28/06/2011**	Sergio Franco	No se introducen cambios tras su revisión. Se actualiza el punto 2. REFERENCIAS
4.0	**14/01/2014**	Sergio Franco	Se introducen cambios de redacción.
5.0	**14/10/2015**	Sergio Franco	Se incluyen en este documento el resto de políticas que conforman el SGSI

INDICE

1. OBJETO Y ALCANCE

La evolución tecnológica ha provocado que las Tecnologías de la Información y Comunicaciones desempeñen un rol estratégico dentro de los procesos claves de las Organizaciones. Bajo este concepto, es necesario considerar la vital importancia que adquiere la información procesada por los recursos tecnológicos y humanos que forman parte de una empresa. Es por ello que se hace necesario establecer políticas que garanticen la seguridad de la información puesto que se trata del activo más importante de las empresas.

El objeto del presente documento es la declaración de las Políticas de Seguridad del Sistema de Gestión Seguridad de la Información de Rallo Hermanos S.A.. Estas Políticas de Seguridad se desarrollan posteriormente en Normativas, Procedimientos e Instrucciones específicas y se verifica su implantación mediante registros y auditorías.

Este documento se articulará a través del propio Sistema de Gestión de Seguridad de la Información basado en la norma internacional ISO/UNE 27001 tratando de forma más detallada todos los aspectos necesarios para la correcta gestión de la seguridad de la información de la Organización.

El alcance del proyecto se encuentra definido en el documento llamado “SGSI-SIS-001-*Alcance del Sistema*”.

2. REFERENCIAS

Esta Política está ampliada y respaldada por los siguientes documentos del SGSI:

OTROS DOCUMENTOS DEL SGSI	
Código	**Documento**
SGSI-SIS-001	Alcance del Sistema
SGSI-SIS-002	Metodología de Análisis de Riesgo
SGSI-REG-AR-R01	Análisis de Riesgo
SGSI-REG-AR-R02	Tratamiento de Riesgo
SGSI-SIS-005	Declaración de Aplicabilidad
SGSI-SIS-006	Manual de Gestión del SGSI

3. PRINCIPIOS Y OBJETIVOS DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Rallo Hermanos S.A. como empresa de logística que lleva años dando servicios a clientes, es consciente de la importancia que adquiere la Seguridad de la Información para las actividades de negocio de la propia organización y de los servicios que ofrece.

Es por ello que Rallo Hermanos S.A. ha implantado un *Sistema de Gestión de Seguridad de la Información* (*SGSI*) basado en la norma internacional ISO/UNE 27001 que garantiza todos los aspectos de seguridad de la información, en términos de confidencialidad, integridad y disponibilidad de la información, relacionados con sus procesos de negocio, servicios ofrecidos a sus clientes y cualquier otra actividad relacionada con la operativa de la compañía. La presente Política establece los objetivos de seguridad de la Organización y se desarrolla mediante normativas, procedimientos e instrucciones técnicas para obtener los objetivos globales de seguridad exigidos.

La política de Rallo Hermanos S.A. se apoya en:

- La aplicación de una Metodología de Análisis y Gestión de Riesgos, definida por la Organización y aprobada por la Dirección, para identificar, evaluar y tratar los riesgos a los que está expuesta en base a criterios previamente definidos por la Metodología y cumplir sus objetivos de negocio.
- Protección el conjunto de la información de la Organización contra incidencias internas y externas, accidentales o no.
- Aseguramiento de que :
    - La información está protegida contra los accesos no autorizados.
    - Se mantiene la confidencialidad, la integridad y la disponibilidad de la información.
    - Se cumplen los requisitos legales, los impuestos por la Organización y por las partes interesadas.
    - Se desarrollan planes de formación a los empleados.
    - Se diseñan las estrategias de continuidad del negocio ante contingencias.
    - Se detectan y reportan todas las vulnerabilidades del sistema para evitar incidencias.

- Existencia de procedimientos que definen las pautas de actuación y de registros que lo evidencian.

Con todo ello, Rallo Hermanos S.A. establece y aprueba unos **objetivos** en Seguridad para el logro de :

- **Mejora interna.** Rallo Hermanos S.A. es consciente de la importancia que tiene la mejora continua de sus procesos internos con el objeto final de proteger la información estratégica de la compañía, de los clientes y de los colaboradores.
- **Mejora de los servicios ofrecidos.** Rallo Hermanos S.A. establece una relación estrecha con todos sus clientes garantizando la aplicación de todas las medidas de seguridad necesarias para preservar la confidencialidad, integridad y disponibilidad de la información en todos los servicios ofrecidos caracterizados por su alta calidad y eficacia, principal argumento en el cual se ha cimentado la confianza de sus clientes desde el nacimiento de la compañía.

La Gerencia de la compañía conoce y aprueba las políticas y normativas de seguridad establecidas declarando que todo el personal de la compañía debe conocer sus responsabilidades en materia de seguridad de la información y aplicar las normativas de seguridad establecidas, como parte de sus funciones de trabajo obligatorias dentro de la Organización.

Para la aplicación efectiva de las políticas y normativas establecidas en el ámbito del SGSI de Rallo Hermanos S.A. se habilitarán los recursos necesarios, estableciendo un Comité de Seguridad y un Responsable de Seguridad, encargados de velar por el satisfactorio cumplimiento de las responsabilidades establecidas, de la revisión de la Política y actualización al menos anualmente; de su publicación; de las acciones auditoras que sean requeridas; y de la atención y resolución de las Incidencias de Seguridad que pudieran tener lugar.

4. CONSIDERACIONES GENERALES

USO ADECUADO DE LAS TIC.

Las políticas definidas en este documento están relacionadas con los activos que manejan información y que son asignados a usuarios, el CPD (Centro de Procesos de Datos), aspectos relacionados con la propiedad de la información que es creada y manipulada por los usuarios y la utilización inadecuada de los recursos que la Organización pone a disposición de los empleados para que desarrollen sus actividades.

CONTRASEÑAS

El cumplimiento de las políticas de contraseñas por parte de los empleados de RALLO es extremadamente importante ya que constituyen la primera línea de defensa para garantizar que la información solo sea accedida por el personal autorizado. Tanto equipos, sistemas y datos utilizan mecanismos de contraseñas para controlar el acceso. No existe ningún control que pueda prevenir el acceso no autorizado a la información si un usuario viola esta política, de ahí su relevancia.

CORREO ELECTRÓNICO E INTERNET

Internet se ha convertido en una herramienta imprescindible en el ámbito profesional de uso prácticamente diario y habitual para cualquier puesto de trabajo. Pero a la vez también puede ser fuente de amenazas invisibles que pongan en riesgo la integridad, la disponibilidad y la confidencialidad de la información que maneja la Organización. Es por ello que desde RALLO Hnos, se ha establecido una política de uso que es de obligado cumplimiento para los empleados que utilicen los medios de los que dispone la empresa para el acceso a Internet

5. POLÍTICA PARA EL USO ADECUADO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES.

Como despliegue de la Política General de Seguridad descrita en el punto anterior, RALLO HNOS, S.A. ha definido otras políticas de menor nivel que informan de manera más detallada a las partes interesadas para facilitar su cumplimiento. No se trata de redactar procedimientos operativos o instrucciones de trabajo, sino directrices definidas por la alta dirección para alertar a los intervinientes y participantes del SGSI de la importancia del cumplimiento de los requisitos establecidos.

Bajo ninguna circunstancia los empleados de RALLO Hnos, pueden utilizar los recursos que la empresa les facilita para realizar actividades prohibidas, ilícitas o que dañen la imagen de la Organización.

5.1.- POLITICA DE CONTROL DE ACCESOS

Como punto de partida para una adecuada implantación de un sistema de seguridad, se establece el control de la seguridad física de acceso a los sistemas automatizados de gestión de información, así como a la propia información que pueda haber en papel o similar. Para ello establece RALLO HNOS, S.A. establece que:

- Los sistemas de gestión de la información tienen el acceso físico restringido mediante el uso de medios de identificación electrónicos que registran cualquier intento de acceso y que dichos accesos se monitorizan regularmente.
- La documentación en papel está debidamente protegida del acceso en función de la criticidad de la información que contiene.
- Existe un puesto de control de accesos que registrará las visitas y solicitará autorización para permitir su entrada.
- El personal de RALLO Hnos. S.A. será el responsable guiar a las visitas que reciba únicamente por las zonas autorizadas. Las visitas únicamente podrán acceder a recepción, salas de reunión o despachos con el acompañamiento del personal de RALLO Hnos.S.A.

- El acceso de personal ajeno a la Organización a zonas con información sensible estará permanentemente supervisado por una persona con responsabilidad dentro del organigrama de la Organización
- Existen niveles y horarios de acceso para todo el personal del grupo Rallo.
- Cualquier visita fuera del horario establecido estará debidamente autorizada por la Dirección de la Organización y queda totalmente prohibido el paso de personal no autorizado.
- Se han establecido sistemas de protección de las instalaciones que impiden el acceso sin autorización por lugares diferentes a los destinados para ello.

5.2.- POLITICA DE COPIA DE SEGURIDAD Y CONTINUIDAD DEL NEGOCIO

Para la subsistencia de cualquier empresa frente a contingencias imprevistas es necesario establecer los principios que rigen la continuidad del negocio.

Rallo Hnos, S.A. basa su plan de continuidad del negocio en los siguientes principios

- Disposición de personal debidamente formado para llevar a cabo las tareas del personal adyacente.
- Contactos con proveedores de servicio de transporte para su subcontratación en caso de necesidad.
- Copias de seguridad de la información
    - La documentación en papel, será digitalizada y formará parte de la información contenida en los planes de copia.
    - Se utilizarán al menos dos medios de copia para los datos sensibles, uno de rápido acceso para contingencias leves y otro para casos más graves.
    - Existirán dos copias fuera de las instalaciones y custodiados por la Dirección de la Organización y la Dirección de Sistemas.
    - Las copias de seguridad fuera de las instalaciones estarán debidamente custodiadas y protegidas para salvaguardar su confidencialidad e integridad.

- Disponibilidad de instalaciones y sistema informático alternativo en caso de desastre mayor.
- Pruebas periódicas de la eficacia del plan que pueden derivar en cambios del mismo en función de los resultados o de nuevos riesgos que se detecten.

5.3.- POLITICA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PUESTO DE TRABAJO.

Todo el personal propio de la Organización, así como proveedores de servicio, pueden tener acceso a información o equipos informáticos durante el desarrollo de sus tareas. Rallo Hnos, S.A., ha establecido una serie de controles para que el personal (propio o subcontratado) solo acceda a los activos estrictamente necesarios y para que sean utilizados debidamente. Para ello Rallo Hnos, S.A. :

- Ha implantado una política de mesas limpias, que obliga al personal a mantener su mesa libre de información al finalizar su jornada o en ausencias prolongadas.
- Dispone de ubicaciones de acceso controlado y restringido.
- Dispone de perfiles de usuarios diferenciados y controla el acceso a los sistemas informáticos mediante contraseñas robustas.
- Ha implantado medidas de seguridad y control para evitar el uso de soportes extraíbles y ha informado a los empleados sobre la prohibición de obtención de información por medios ilícitos.
- Forma a sus empleados e informa a los subcontratistas sobre el manejo de la información a la que tienen acceso.
- Dispone de unas cláusulas de confidencialidad en los contratos de trabajo o contratos de prestación de servicios que deben entendidos y llevados a cabo por el personal.
- Supervisa de forma directa cualquier actuación de terceros que suponga un acceso a los activos que contengan información.
- Las actualizaciones de programa de gestión será verificada en un entorno de pruebas antes de validar su instalación en el sistema real.

Tanto desde la Dirección de Sistemas, como desde la Dirección de la Organización, se promoverán las buenas prácticas en materia de seguridad de la información y se asegurarán que los empleados, propios o subcontratados, las ponen en práctica, además de requerirles que informen de cualquier vulnerabilidad o debilidad que detecten durante el desarrollo de sus actividades. Así pues RALLO Hnos, notifica a los usuarios que está totalmente prohibido:

- Violar los derechos de cualquier persona o institución protegidos por derecho de autor, patentes o cualquier otra forma de propiedad intelectual.
- Difundir información identificada como confidencial a través de cualquier medio
- Introducir software malicioso en la red o en los servidores (virus, worm, spam, …
- Utilizar la infraestructura TIC de RALLO Hnos para conseguir o transmitir material con ánimo de lucro, realizar acosos, difamación, calumnia o cualquier forma de actividad hostil.
- Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios de RALLO Hnos.
- Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.
- Ejecutar mecanismos de monitoreo de red no autorizados expresamente por la Dirección de Sistemas.
- Burlar mecanismos de seguridad, autenticación, autorización o auditoría de cualquier servicio informático.
- Descargar archivos no relacionados con la actividad profesional (software malicioso, múltimedia….)

Por motivos de mantenimiento de red, de seguridad, de eventos programados, de pruebas, …. determinados cargos con responsabilidad podrán quedar exentos de seguir algunas de las restricciones aquí indicadas siempre por motivos justificados y que deberán notificarse previamente a la Dirección de Sistemas.

5.4.- POLITICA DE USO DE TERMINALES MÓVILES.

Las nuevas tecnologías permiten el uso de información en terminales móviles de telecomunicaciones. Es por ello que surge la necesidad de establecer los criterios de uso seguro de estos terminales. En concreto la Organización establece que :

- El uso de los dispositivos móviles propiedad de Rallo Hnos, es exclusivo para temas profesionales relacionados con cada puesto de trabajo.
- Bajo ninguna circunstancia, los empleados de RALLO Hnos, pueden utilizar los recursos informáticos para llevar a cabo actividades ilegales.
- No está permitida la instalación de programas que no hayan sido autorizados por la Dirección de la Organización o por la Dirección de Sistemas.
- Se deberá impedir el acceso al terminal a terceras personas, manteniendo una custodia adecuada del equipo y habilitando sistemas de control de acceso (pantalla de bloqueo, código pin, huella digital....).
- Se habilitarán los sistemas de localización de los terminales para poder acceder a ellos en caso de pérdida o robo.
- Cualquier incidencia del terminal será notificada inmediatamente al responsable de sistemas para que proceda a realizar las acciones oportunas en aras a mantener la seguridad de la información.
- El soporte técnico o la configuración de equipos no podrá ser realizado por terceros sin la autorización expresa de la Dirección de la Organización.

5.5.- POLITICA DE USO DE INTERNET Y EL CORREO ELECTRÓNICO

.Rallo Hnos, S.A. facilita el uso de internet y correo electrónico a sus empleados para que los utilicen convenientemente para el mejor desarrollo de sus tareas. Los servicios de acceso a Internet y al correo electrónico son administrados por el Departamento de Sistemas, quien está facultado para monitorear la actividad de cada usuario con la finalidad de:

- Verificar el cumplimiento de las políticas del Sistema de Gestión de la Seguridad de la Información,
- Detectar deficiencias en la prestación del servicio tanto a nivel interno como externo (Proveedor de telecomunicaciones) que puedan derivar en incidencias.
- Buscar evidencias ante cualquier incidencia.

Los principios que rigen la política de uso del correo electrónico son los siguientes:

- El usuario es responsable del contenido de los mensajes enviados.
- Se prohíbe la transmisión de mensajes con contenido ofensivo u obsceno, ilegal, discriminatorio, despectivo, malintencionado, cadenas de correo, spam, publicidad engañosa, … y en general cualquier tipo de información que cause congestión de red o interfiera en el trabajo de otros.
- El Departamento de Sistemas bloqueará de forma automática la recepción de correos electrónicos que provengan de fuentes de correo basura, virus o códigos maliciosos.
- El Departamento de Sistemas bloqueará el envío y recepción de determinados tipos de ficheros adjuntos que puedan suponer un riesgo para el sistema de seguridad de la información (exe, bat, js, …)
- El Departamento de Sistemas determinará el tamaño máximo permitido para el envío y recepción de documentos adjuntos para evitar colapsar el servidor de correo.
- Se prohíbe abrir archivos adjuntos cuyo origen se desconozca sin la autorización de la Dirección de Sistemas. Aún siendo el origen conocido, si el adjunto no se corresponde con lo esperado, el usuario deberá consultar con el Dirección de Sistemas.
- Si se detecta la entrada de publicidad no solicitada y molesta, se informará al Departamento de Sistemas para su análisis y solución.
- El usuario no debe facilitar la dirección de correo profesional para temas personales (alta de servicios, compras por internet, ….)

Y por otro lado, los principios que rigen la política del uso de Internet son:

- El acceso a Internet a través de los equipos de RALLO Hnos, será por motivos laborales y profesionales.
- No está permitido el uso del acceso a Internet como medio de participación, acceso y distribución de actividades o materiales que supongan una infracción legal.

- Queda prohibido el acceso, descarga o transmisión de material cuyo origen no sea constatado como seguro o que se desconozca su confiabilidad.
- Queda prohibida la navegación por páginas inapropiadas para el normal desarrollo de la actividad.

5.6.- POLITICA DE CONTRASEÑAS.

- Todo el personal de RALLO Hnos, que accede al Sistema Informático deberá disponer de un nombre de usuario y una contraseña.
- Para su primera conexión, el administrador del sistema le otorgará una contraseña que será sólo válida para establecer la suya propia.
- Las contraseñas de los usuarios cumplirán con determinados requisitos de complejidad para evitar contraseñas débiles.
- Las contraseñas son personales y conocidas únicamente por el propio usuario, quien será responsable de cualquier actividad que se realice con ella. Ni siquiera el administrador del sistema puede tener acceso a las contraseñas del resto de usuarios.
- El usuario podrá cambiar su contraseña, con algunas restricciones, siempre que quiera, siendo obligado hacerlo cada cierto periodo de tiempo definido por el administrador del sistema.
- El Administrador del Sistema se reserva el derecho a restablecer la contraseña de cualquier usuario por motivos de seguridad
- Las sesiones se bloquearán automáticamente transcurrido un periodo de tiempo de inactividad y será necesaria la introducción de la contraseña para desbloquearlas.
- Las contraseñas de las cuentas de correo no serán notificadas a los empleados para evitar la configuración de cuentas en dispositivos no controlados.
- Queda terminantemente prohibido:
    - Revelar las contraseñas a personal no autorizado
    - Anotar la contraseña en zonas accesibles y/o visibles.
    -

5.7 POLÍTICA DE EQUIPOS TIC

- Los equipos informáticos propiedad de RALLO Hnos, deberán ser utilizados únicamente para actividades relacionadas con los objetivos y metas de la Organización.
- Las compras de equipos para el tratamiento de información se realizarán siguiendo una planificación que incluya un análisis de riesgos y que permita adoptar las medidas necesarias para la minimización del impacto.
- Para el correcto funcionamiento del equipo, el departamento de sistemas diseñará y llevará a cabo un plan de mantenimiento de los mismos, tanto a nivel hardware, como a nivel software.
- Solo el Departamento de Sistemas está facultado para realizar tareas de mantenimiento. La contratación de terceros para la reparación, mantenimiento, instalación … será aprobada por Gerencia y supervisada directamente por el Departamento de Sistemas para mantener los niveles de seguridad de la información.
- El Departamento de Sistemas mantendrá los sistemas operativos de los equipos debidamente actualizados con las últimas versiones de los mismos.
- Los usuarios de cada equipo son los responsables del buen uso del mismo, notificando al departamento de sistemas cualquier incidencia que detecten para que sea resuelta en el menor tiempo posible.
- La pérdida o robo de un equipo deberá ser notificada inmediatamente al Departamento de Sistemas por la vía más rápida.
- Queda prohibida la conexión de cualquier tipo de equipo a la red de RALLO Hnos, salvo autorización expresa del Departamento de Sistemas.

5.8.- POLÍTICA DEL CENTRO DE PROCESO DE DATOS (C.P.D)

El Centro de Proceso de Datos, también conocido como CPD o Sala de Servidores, es la sala donde se encuentran físicamente los servidores y demás equipos de control del sistema informático. Dicha sala cuenta con:

- Control de Accesos: Acceso permitido solo al personal definido por la Dirección de RALLO Hnos.
- Sistema redundante de refrigeración: La sala cuenta con dos equipos de aire acondicionado que mantienen la temperatura de la misma en valores próximos a 17ºC
- Presencia de SAIS: Existe un SAI general que alimenta todo el edificio de oficinas y sala de control de accesos y dos SAIS adicionales para el RACK de comunicaciones.

El uso de la sala queda limitado únicamente al personal que tiene el acceso permitido. El acceso de un tercero deberá ser autorizado por la Dirección de la Empresa o por la Dirección de Sistemas y durante su estancia en la misma, estará siempre acompañado por el personal que se designe. Bajo ningún concepto puede quedar nadie no autorizado dentro de CPD sin acompañamiento de un autorizado.

Dentro del plan de mantenimiento del Sistema informático se verificará el correcto funcionamiento de los equipos auxiliares instalados en el CPD, así como la ausencia de elementos que no estén relacionados con la actividad propia de la sala.