AVISO LEGAL

INFORMACIÓN DE USO INTERNO

La información aquí contenida es de La Compañía. Su distribución, divulgación, reenvío, copia, impresión, reproducción y uso por parte de terceros ajenos o externos a las Compañías, requiere la autorización expresa.

INFORMACIÓN RESTRINGIDA Y CONFIDENCIAL

La información aquí contenida es de La Compañía. Contiene información legalmente protegida por ser privilegiada o confidencial. Cualquier distribución, divulgación, reenvío, copia, impresión, reproducción o uso indebido de esta información, sin la autorización expresa por escrito de las Compañías está estrictamente prohibida y será sancionada legalmente.

OBJETIVO

Brindar un nivel de protección adecuado a la solución contratada, que permita reducir los riesgos de seguridad a un nivel aceptable por nuestra Compañía, con base en los requerimientos organizacionales para la protección de los datos y el modelo de seguridad; y considerando, los requerimientos legales y regulatorios, los objetivos de control, los principios, políticas, reglas, estándares y procedimientos establecidos a nivel interno.

ALCANCE

Este documento se aplica a todas las instancias en las cuales individuos, organizaciones o empresas externas requieran acceso a los sistemas de información digital de la compañía.

RESPONSABLE

Especialista seguridad de la información

CONTENIDO

Aspectos Generales:

- Cuando sea prestación de un servicio el contratista debe enviar mensualmente el certificado de pago a la seguridad social y certificados de trabajos en alturas si aplica.
- Garantizar el control de activos asignados al proveedor antes, durante y después del servicio prestado
- Garantizar el registro y control a áreas restringidas de ARUS.
- Mantener actualizados los accesos suministrados para la prestación del servicio, los cuales no deben ser compartidos ni divulgados.
- Conocer y cumplir las políticas de seguridad de información y salud en el trabajo de la Compañía ARUS.
- Informar cualquier anomalía que identifique en el desarrollo de su servicio.
- La información digital y física custodiada por personal externo a ARUS y que se encuentre por fuera de las instalaciones, debe contar con un esquema de respaldo y controles de seguridad. Adicionalmente, se cuenta con acuerdos de servicio establecido en las ofertas mercantiles o contratos entre las partes (Proveedores de Data Center), referente a la realización del Back Up y la custodia de los mismos para garantizar la disponibilidad, integridad y confidencialidad de la información
- Cualquier incumplimiento en los lineamientos descritos en este documento pueden generar acciones de acuerdo con lo definido contractualmente.

Seguridad Física

- La Organización cuenta con rutas y salidas de emergencia, las cuales deben utilizarse sólo en estos casos o bajo instrucciones del equipo de emergencias (descrito en el Plan de Emergencias).
- Todos los terceros que ingresen a cualquier instalación de la Compañía deben portar carné o identificación y estar acompañados por un responsable de la organización.
- El acceso a zonas seguras sólo está permitido para motivos específicos y relacionados a actividades estrictamente laborales y el personal que ingrese a dichos sitios siempre debe estar acompañado del responsable de la zona y registrarse en la planilla dispuesta para este fin.
- No se permite comer, consumir sustancias alcohólicas o psicoactivas, fumar dentro de las instalaciones de la organización, zonas de procesamiento de información o en sitios donde estén expuestos equipos electrónicos.
- Todas las puertas de aislamiento de Zonas Seguras deben permanecer cerradas, razón por la cual el responsable de dicha zona debe asegurarse de esto al abandonar el sitio.

Recursos Humanos

- El líder del proceso responsable de su labor debe darle a conocer las directrices de seguridad en materia de: Seguridad y Salud en el trabajo, plan de emergencias, plan de continuidad del negocio y accesos permitidos para sus labores. Así mismo, esta responsabilidad incluye las sanciones frente a los incumplimientos y fraudes definidos en el contrato.
- El proveedor debe garantizar controles de seguridad para la selección de sus empleados que garanticen la seguridad de la información a la cual van a tener acceso.
- Se debe garantizar la firma de acuerdos de seguridad con sus empleados y clausulas asociadas al tratamiento de la información crítica proveniente de la ejecución de sus labores.
- Garantizar la devolución de los activos asignados, así como la cancelación de accesos lógicos y físicos.

Adquisición y Mantenimiento Sistemas

Control de Software

- Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.
- Únicamente está permitido el uso de software licenciado y adquirido por la organización, o bien, del desarrollado por la misma, con la previa autorización de la Gerencia de Tecnología.
- Realizar monitoreo periódico al software instalado en las máquinas de proveedores/ contratista.

- La organización supervisa y monitorea el desarrollo del software subcontratado por medio de un líder de desarrollo. La tercerización en el desarrollo de Software, incluye los requisitos contractuales y legales que aseguran la propiedad sobre los derechos del software y la seguridad del mismo con las partes externas, como se muestra en la Guía de Cumplimiento perteneciente a la presente política.

Cumplimiento

Derechos de autor

- Únicamente pueden utilizar material autorizado por la organización. En caso de utilizar documentación proveniente de entes externos, es necesario aplicar etiquetas o marcas claras que haga referenciación a la identificación del propietario intelectual de dicha información.
- Así mismo, se debe respetar los derechos de Autor para la información utilizada con algún propósito que aplique a la organización, justificando claramente la fuente de proveniencia de la información.
- No está permitido coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que pueda infringir o violar cualquier patente, derechos de autor, marcas, secretos empresariales o cualquier otro derecho intelectual de otra persona u organización, es decir, cualquier acción que viole los acuerdos de licencias del software instalado o de derechos de autor.
- El incumplimiento de estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

Propiedad intelectual

- Todos los empleados y proveedores involucrados en el desarrollo deben firmar la cesión de derechos patrimoniales para dar propiedad del desarrollo a la compañía, para el caso específico de proveedores, debe quedar explícito en la contratación que la propiedad intelectual pertenece a la Compañía y no a quien ejecuta el encargo.

Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

- Los recursos de procesamiento de información de la organización se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos se considera como uso indebido.
- Tener acceso únicamente a la información necesaria para el desarrollo de su trabajo y reportar inmediatamente cuando tenga más accesos de los que le corresponden.
- Todos los terceros, proveedores y/o contratistas deben conocer el alcance preciso de las funciones de su cargo y las herramientas tecnológicas necesarias para ejecutar las tareas del mismo, lo cual es responsabilidad del líder que administra el tercero, proveedor y/o contratista.

- Abstenerse de divulgar información en forma verbal, escrita, telefónica o electrónica, que esté clasificada como confidencial, restringida o interna en la Compañía. Ésta solo debe realizarse sobre la base de la necesidad de conocerla de acuerdo a sus funciones.
- Imprimir información clasificada como confidencial, restringida o interna de la Compañía, bajo condiciones de seguridad. Ej.: Hacer uso de claves en las impresoras, recoger inmediatamente los documentos de las impresoras o fotocopiadoras, etc.

Seguridad de la Información

Comunicación de Incidentes Relativos a la Seguridad

- Reportar oportunamente los eventos y debilidades de las que tenga conocimiento y que puedan poner en riesgo la seguridad de la información de la organización. Ej.: Comportamiento inadecuado con relación al manejo de usuarios y contraseñas, equipos desatendidos, ingresos a sitios no autorizados, etc.
- Todos los terceros, proveedores y/o contratistas de la Compañía son responsables de garantizar la seguridad de la información, por lo cual los incidentes relativos a la seguridad lógica deben ser comunicados de manera oportuna a los responsables y asegurarse que el personal necesario haya sido enterado del caso.

Control de Accesos

- Con el objetivo de impedir el acceso no autorizado a la información, la compañía cuenta con el procedimiento para la Gestión de Accesos lógicos, perteneciente al proceso de Seguridad de la Información. Las directrices aquí expuestas controlan la asignación de derechos de acceso a los sistemas, datos y servicios de información.
- No se permite compartir usuarios de acceso a los sistemas de la Compañía.
- Todos los usuarios deben cambiar 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 se suministran una vez identificado el usuario.
- Para el ingreso a sistemas y aplicativos de su organización en los cuales custodie información de nuestra Compañía, debe contar con políticas de vencimiento de contraseñas y bloqueo por exceder cantidad de intentos fallidos.
- Proteger sus cuentas de usuario y contraseñas de acceso a la información, para evitar que sean expuestas o utilizadas por personas no autorizadas. Recuerde que éstas son personales e intransferibles.
- Está prohibido dejar escritas las contraseñas en lugares públicos o vistosos, que permitan el acceso no autorizado de otras personas.
- Se debe solicitar o realizar el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Se debe evitar la inclusión de contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función, autoforma o macro.
- Está prohibido compartir los usuarios y contraseñas de acceso a cualquier sistema de la compañía el personal será responsable por todas las actividades realizadas con los

usuarios y contraseñas entregados por la compañía para el acceso a los sistemas de información.
- Debe informar oportunamente a Arus sobre la necesidad de modificar o cancelar derechos de acceso asignados para la prestación del servicio.

Equipos Desatendidos

- Todos los miembros de la organización deben garantizar que los equipos desatendidos estén protegidos adecuadamente.
- Abstenerse de dejar desatendidos los medios físicos y/o electrónicos que contengan información confidencial, restringida o interna definida por nuestra Compañía.

Control de Acceso a la Red

Utilización de los Servicios de Red

- Las conexiones no seguras a los servicios de red pueden afectar a toda la organización, por lo tanto, se controla el acceso a los servicios de red tanto internos como externos, con el fin de garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos. Por este motivo, las redes (incluidas las inalámbricas) están protegidas mediante el filtrado de páginas web con contenido no laboral.

Acceso a Internet

- No está permitido el ingreso a páginas con contenido no laboral.
- Los usuarios sólo deben acceder a los servicios para cuyo caso estén específica y previamente autorizados.
- No se autoriza el uso de servicios de mensajería instantánea distinta a la entregada o autorizada por la Compañía.
- No se autoriza el uso de servicios de vídeo conferencias distintas a las ofrecidas por la Compañía y para cargos que así lo requieran como parte de sus labores.
- La descarga de contenido multimedia se permitirá únicamente a los cargos que lo necesiten para el desempeño de sus labores.

Sistema de administración de contraseñas

- El sistema de administración de contraseñas debe estar configurado para:
  - Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
  - Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo, claves de impresoras, Hubs, routers, etc.).
  - Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

Equipos Portátiles y Trabajo Remoto

- Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información de la organización.
- Evitar la conexión a redes catalogadas como no seguras o que no proporcionen el nivel de confidencialidad que necesita la organización (por ejemplo redes inalámbricas ajenas).
- Debe evitar abrir archivos sospechosos o de remitentes desconocidos ya que estos pueden venir infectados con virus, software espía, gusanos, malware o códigos maliciosos, los cuales pueden ser transferidos a la red Corporativa.
- Debe tenerse en cuenta que los computadores portátiles no deben ser aforados por ningún motivo como equipaje de bodega.
- En los casos, donde el dispositivo móvil se ha perdido o ha sido robado, es importante contar con la posibilidad que la información confidencial contenida en dicho equipo no sea accedida por terceros, por lo cual es importante asegurar dichos equipos electrónicos con claves de arranque, claves de acceso de administrador y claves personales de bloqueo de teclado que tengan el mismo tipo de características de configuración como se explica en el numeral relacionado a contraseñas.
- Para la utilización de dispositivos móviles, los empleados deben seguir las siguientes recomendaciones:

    a) Permanecer siempre cerca del dispositivo.
    b) No dejar desatendidos los equipos.
    c) No llamar la atención acerca de portar un equipo valioso.
    d) No poner identificaciones de la compañía en los dispositivos, salvo los estrictamente necesarios.

- Para la ejecución de actividades en modalidad remota, se debe tener en cuenta las siguientes recomendaciones:
    - La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.
    - Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.
    - La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar.

Manejo de activos de información

- Todos los proveedores/contratistas son responsables de salvaguardar y cuidar los activos de información que la organización ha entregado para sus labores dentro o fuera de los límites físicos de la misma (equipos tecnológicos y no tecnológicos, procesos, instalaciones).
- Por ningún motivo se permite la divulgación y extracción de información confidencial y privada de la Compañía o Clientes.

- Acatar los criterios de clasificación de la información, definidos en el Modelo de Información de ARUS para realizar un tratamiento adecuado de la información.

Eliminación de activos:

- Los discos duros y equipos de cómputo que contengan información de la compañía, deben ser formateados antes de ser dispuestos en sitios de desecho.
- Se debe garantizar la eliminación de cualquier información que se encuentre almacenada en la memoria de estos equipos y realizar una relación de devolución mediante un acta en la cual se registre el serial del equipo devuelto.
- Para la disposición física de medios removibles tales como USB, CD, DVD, discos duros portátiles externos o discos duros contenidos dentro de PC's, debe realizarse un procedimiento de borrado lógico y posteriormente realizar la destrucción física a través de técnicas que apoyen la conservación del medio ambiente

Gestión de Comunicaciones y Operaciones

Definir e implementar los controles para disminuir los riesgos en el Software, teniendo en cuenta los siguientes ítems:

- Instalar y actualizar periódicamente software de detección y reparación de virus, examinando los medios informáticos, como medida preventiva.
- Mantener los sistemas con actualizaciones de seguridad recientes según las necesidades del negocio.
- Realizar mantenimiento periódico a las aplicaciones críticas del negocio, o según lo amerite.
- Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes o medios no confiables.
- Generar estrategias de comunicación para fomentar buenas prácticas en el uso del software y prevención de código malicioso.

Resguardar cada software o dato en función de su criticidad.

Los sistemas de resguardo son probados periódicamente, asegurando que cumplen con los requerimientos de los planes de continuidad de las actividades de la organización.

El resguardo de la información considera:

a) La marcación de las copias de resguardo, que permite identificar de manera adecuada la información contenida.
b) Almacenamiento en una ubicación diferente las copias recientes de información, según aplique.
c) Los medios magnéticos deben ser almacenados en áreas seguras y bajo condiciones ambientales adecuadas.
d) Se prueban periódicamente los medios de resguardo

Controles de Redes

Se debe controlar la seguridad de los datos y los servicios conectados en las redes de ARUS contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Establecer los controles para la administración remota de los dispositivos que pertenezcan a la red.
b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.
c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

El intercambio de información entre la organización y las partes interesadas se realiza por canales y medios seguros. Adicionalmente, se tienen en cuenta los aspectos legales y contractuales para este intercambio según aplique a la operación de los productos.

Continuidad de Negocio

En caso que el servicio prestado por proveedor/contratista sea considerado crítico para ARUS, estos deben garantizar estrategias de continuidad del negocio de acuerdo al alcance y servicio contratado.

Protección de datos

- Toda la información que sea entregada por ARUS debe ser gestionada por el proveedor cumpliendo las normas y leyes asociadas a la protección de datos.
- El proveedor debe garantizar controles para la protección de bases de datos a las que pueda acceder de ARUS S.A.S o nuestros clientes y entregar a ARUS S.A.S. copia de su política de Protección de Datos Personales cuando sea necesario para el servicio que preste.
- La información entrega por ARUS no podrá ser utilizada para ningún fin diferente al contratado.
- El proveedor debe reportar a ARUS cualquier evento de seguridad que afecte la disponibilidad, integridad y confidencialidad de la información entregada.

CONTROL DE CAMBIOS

Versión	Descripción del cambio	Realizado por	Fecha
1	Se realizan ajustes de acuerdo a lineamientos de nueva marca. Ver Acta de Control de Cambios Nueva Marca	Equipo Gestión por Procesos	06/10/2016
2	Actualización de cargos por cambios de estructura	Coordinador de riesgos y control	22/05/2020
3	El tercero debe notificar oportunamente a Arus sobre los cambios o retiro de accesos que le fueron asignados	Coordinador de Seguridad de la Información	22/06/2021
4	- Se crea objetivo y responsable de la política - Se ajusta alcance del documento, excluye Enlace Operativo - En numeral Seguridad Física, se elimina numeral sobre prohibición de ingreso de equipos electrónicos a las áreas de procesamiento de información crítica - Se actualizan numerales: Adquisición y Mantenimiento Sistemas, Derechos de autor y Acceso a Internet	Especialista de seguridad de información y Analista Control de Accesos Aprobado por: Director TI Interna	14/05/2024

ANEXOS N/A