OBJETIVO

Establecer los lineamientos para la administración y seguridad de los activos de información de Compañía de Empaques S.A y sus filiales, almacenados tanto en cada uno de los programas y/o aplicaciones, equipos fijos, móviles y servidores y archivos físicos de la organización, propendiendo por la seguridad y el cuidado de dicha información, frente a perdidas, fugas y daños involuntarios o voluntarios en la misma.

ALCANCE

Aplica para Compañía de Empaques S.A y todas sus filiales, así como incluye a cada uno de los funcionarios que usan la información.

LINEAMIENTOS OPERACIONALES DE SEGURIDAD DE LA INFORMACIÓN

PROTECCIÓN DE LA INFORMACIÓN

Todo activo de información, especialmente aquella que contenga datos personales de terceros (clientes, proveedores, empleados), se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Se establecerá un **Oficial de Seguridad de la información o un funcionario que haga sus veces**, el cual será responsable del tratamiento de la información en los componentes tecnológicos y físicos acorde a la arquitectura de seguridad o controles existentes para este fin.

Se establecerá un **Comité de seguridad de la Información** el cual estará compuesto por la Vicepresidencia Financiera y Administrativa, La Gerencia de TI, el Oficial de seguridad o quien haga sus veces y Auditoría Interna. (Ver Reglamento Interno del Comité de Seguridad de la Información).

IDENTIFICACIÓN, CLASIFICACIÓN Y CONSERVACIÓN DE LOS ACTIVOS DE INFORMACIÓN.

Se identificarán los activos de información, el sistema de información que lo procesa o almacena, su respectivo propietario y la unidad organizativa a la que pertenece.

Se Clasificarán los activos de información de acuerdo con su sensibilidad y criticidad en: (Ver procedimiento para identificar, clasificar y conservar los activos de la información):

- **Información secreta.**
- **Información sensible.**
- **Información restringida.**
- **Información pública.**

GESTIÓN DE RIESGOS

Se realizará un análisis y valoración de riesgos a todos los activos de la información de acuerdo a la política y procedimiento interno de Gestión del riesgo.

Al realizar el análisis y valoración de riesgos, se deberá considerar los riesgos de los servicios en la nube que la Compañía de Empaques S.A. y sus filiales pudiera contratar.

Tipos de riesgos que se deberían evaluar

Acceso no autorizado de usuarios con privilegios: Este riesgo genera pérdida de confidencialidad, integridad e incluso disponibilidad, aparece, por ejemplo: cuando un empleado con privilegios de administrador accede cuando no debería o actúa de forma maliciosa (empleados descontentos, por ejemplo) alterando datos o configuraciones. También es posible que se den privilegios por error a empleados que no deban tenerlos y estos por desconocimiento provoquen daños.

Incumplimiento normativo: Este tipo de riesgos de la nube puede tener consecuencias administrativas o penales, aparece cuando el proveedor no cumple, o no nos permite cumplir con nuestras obligaciones legales aplicables en cada país, relacionadas con la protección de datos personales y penalización de actos que atenten contra la confidencialidad, integridad y confidencialidad de los datos y de los sistemas de informáticos.

Desconocimiento de la localización de los datos: Cuando se contratan servicios a un proveedor que aloja los datos en un Centro de Datos del cual se desconoce su ubicación, se pone en riesgo la seguridad de estos al desconocer la legislación de otros países. Por ejemplo, si se tratan con datos de carácter personal, es necesario que se proporcionen las garantías jurídicas necesarias sobre la privacidad de los mismos.

Indisponibilidad del servicio en caso de desastre o incidente: Si el proveedor sufre un incidente grave o un desastre y no tiene un plan de continuidad, por ejemplo, los servicios y los datos replicados en otro centro de datos, no podrán seguir dando servicio.

Carencia de soporte investigativo: En caso de que ocurra un incidente, es necesario revisar los accesos a los datos para saber qué ha ocurrido. En este caso, no se podrá actuar si el proveedor no garantiza el acceso a los logs o registros de actividad.

Viabilidad a largo plazo: Existe el riesgo de que las condiciones del contrato sufran alguna modificación debido al cambio de estructura del proveedor, de la alta dirección, a la entrada en situación de quiebra de este o a que decida externalizar parte de sus servicios. Por ello es recomendable asegurarse el acceso a los datos y su recuperación.

API o Servicios WEB: Existe el riesgo de que no se utilicen buenas prácticas de desarrollo y de conexiones seguras en las API's o Servicios Web suministrados por el proveedor de servicios en la nube.

Falta de una estrategia de migración: Se debe contar con la estrategia de migración a otra plataforma en caso de terminación del contrato por cualquiera de las partes, por la interrupción o la degradación en la prestación del servicio de parte del proveedor de servicios en la nube o por cualquier otro motivo que considere razonable la Compañía.

Falta o incompleta documentación: Falta o inadecuada actualización de documentación de procesos, procedimientos, aplicaciones y diagramas de red, de los servicios que se ejecutan en la nube.

Inadecuados niveles de servicios: La Compañía debe mantener actualizada la información que se relaciona los procedimientos para verificar el cumplimiento de los acuerdos y niveles de servicio establecidos con el proveedor de servicios en la nube.

Falta de reportes del nivel de madurez de la seguridad: La Compañía debe mantener actualizada la información que se relaciona con los reportes generales de auditoría, pruebas de vulnerabilidades y estado actual de los servicios contratados.

CONSERVACIÓN DE LA INFORMACIÓN

La conservación de la información será definida por Compañía de Empaques S.A y sus filiales de acuerdo con la clasificación y el análisis de riesgos de ella (por ejemplo, información secreta se puede conservar de 10 a 20 años, información sensible de 5 a 10 años, información restringida de 2 a 5 años e información pública de 1 mes a un año). (Ver procedimiento para identificar, clasificar y conservar los activos de la información):

CONTROL DE ACCESO A LA INFORMACIÓN

Es responsabilidad de los dueños de los activos de información autorizar el acceso adecuado a los activos de información bajo el principio del mínimo privilegio; "acceso mínimo requerido para el normal desempeño de sus labores", para mitigar la fuga o modificación de la información. (Ver procedimiento para identificar, clasificar y conservar los activos de la información):

CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Todos los colaboradores internos y externos de Compañía de Empaques S.A y sus filiales deberán recibir capacitación sobre la seguridad de la información, el uso adecuado de los activos de información, las instalaciones de procesamiento de información y en general sobre los activos de información.

PROTECCIÓN DE LA INFORMACIÓN FÍSICA Y ELECTRÓNICA DURANTE SU CICLO DE VIDA

Cada colaborador de Compañía de Empaques SA y sus filiales es responsable de:

- Acatar los criterios de clasificación de la información, definidos para un tratamiento adecuado de la información.
- Usar la información a la cual tiene acceso, sólo para propósitos del negocio, atendiendo a las responsabilidades definidas en función del rol que desempeña en Compañía de Empaques S.A y sus filiales.
- Tener acceso únicamente a la información necesaria para el desarrollo de su trabajo y reportar cuando tenga más accesos de los que le corresponden.
- Proteger sus cuentas de usuario y contraseñas, para evitar que personas no autorizadas las usen. Éstas son personales e intransferibles.
- Reportar oportunamente los eventos y debilidades de las que tenga conocimiento y que puedan poner en riesgo la seguridad de la información de Compañía de Empaques S.A y sus filiales Ejemplo: manejo inadecuado de usuarios y contraseñas, equipos desatendidos, ingresos a sitios no autorizados, etc.
- Aplicar protección a la información, bien sea porque es el dueño de esta o porque tiene acceso como usuario.
- Administrar eficientemente la información de la cual es responsable, aplicando procedimientos durante el ciclo de vida de esta. Ej.: depurar la información innecesaria para el desarrollo de su trabajo.
- Abstenerse de dejar desatendidos los medios físicos y/o electrónicos que contengan información secreta, sensible o restringida.

- Abstenerse de divulgar información en forma verbal, escrita, telefónica o electrónica, que esté clasificada como secreta, sensible o restringida. Se permite hacerlo bajo la necesidad de conocerla de acuerdo con las funciones del solicitante.
- Imprimir información clasificada como secreta, sensible o restringida, bajo condiciones de seguridad. Ejemplo: usar contraseña en las impresoras, recoger inmediatamente los documentos de las impresoras o fotocopiadoras, etc.
- Usar técnicas de cifrado para información electrónica o sobres sellados para información física, para enviar información clasificada como confidencial, restringida o interna. El envío de medios físicos debe realizarse a través de mensajería certificada, donde se garantice la identificación de éstos.
- Garantizar que, al momento de destruir la información secreta, sensible o restringida en formato físico, no sea recuperable. Ejemplo: usar máquina trituradora.
- Garantizar la seguridad de la información / ciberseguridad que se intercambia a través de medios físicos o electrónicos, a nivel interno y externo.

RESPALDO O COPIAS DE SEGURIDAD DE LA INFORMACIÓN

La Alta Gerencia en compañía con el área de TI, identificaran los responsables de realizar las copias de seguridad y definir el procedimiento para hacer los backups y las restauraciones. (de que hacer copia, periodicidad, ubicación, etc.). Ver: Procedimiento de respaldo de la información y Procedimiento plan de respaldo contingencias TI.

ACCESO A ÁREAS SEGURAS (Ver procedimiento de seguridad física)

Las áreas seguras, centros de datos y rack de comunicaciones, se deben mantener cerrados y con llave. Se deberá realizar una planilla control de autorización, para realizar algún trabajo en dichos sitios, ya que se tienen que entregar las llaves para que puedan acceder a ellos.

Se prohíbe la grabación de vídeo en las instalaciones de áreas seguras de Compañía de Empaques S.A y sus filiales.

Las áreas clasificadas como seguras deben contar con grabaciones del CCTV, con personal encargado de monitorear. Ver Procedimiento de administración de cámaras.

En las instalaciones del centro de datos o de los centros de cableado, NO estará permitido:

- Fumar dentro del Data Center.
- Introducir alimentos o bebidas al Data Center.
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

El centro de datos debe estar provisto de:

- Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
- Pisos elaborados con materiales no combustibles.
- Sistema de refrigeración por aire acondicionado.
- Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
- Alarmas de detección de humo. Los detectores deberán ser probados de acuerdo con las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
- Extintores de incendios cercanos o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.
- El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por personal del área de TI.
- Las puertas del centro de datos deben permanecer cerradas.
- Cuando se requiera realizar alguna actividad sobre algún rack, este debe quedar ordenado, cuando se finalice la actividad.
- Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
- Los equipos del centro de datos que lo requieran deben estar monitoreados para poder detectar las fallas que se puedan presentar. Esta revisión se hace diariamente sobre todos los servidores que se encuentran en sitio.

CONTROL DE ACCESO LÓGICO (Ver Procedimiento para la seguridad de la información)

Control de acceso a plataforma tecnológica

Compañía de Empaques S.A y sus filiales, garantizarán a los colaboradores, todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: computadores portátiles, tablets, enrutadores, agendas electrónicas, celulares inteligentes, access point, entre otros, sin la debida autorización del Oficial de Seguridad de la Información o quien haga sus veces o del área de infraestructura de TI.

Solo TI está autorizado para instalar software y/o hardware en los equipos, servidores e infraestructura de telecomunicaciones de Compañía de Empaques SA y sus filiales, así como el uso de herramientas que permitan realizar tareas de mantenimiento, revisión de software, recuperar datos perdidos, eliminar software malicioso.

Las autorizaciones de sistemas, aplicativos, acceso a servicios de TI, administración de servicios de TI, deben ser solicitados mediante correo sistemas.infraestructura@grupoexcala.com, estos quedan registrados en el sistema de mesa de ayuda de TI (GLPI).

Del mismo modo, para la solicitud de servicios que tengan que ver con el ERP sistemas.analistas@grupoexcala.com.

En cuanto a los accesos a la red, el equipo deberá registrarse, de lo contrario no tiene acceso a ninguno de los recursos. Adicionalmente, todos los usuarios habilitados para trabajar en la red de la Compañía de Empaques S.A y sus filiales deben tener bloqueo para instalar aplicativos.

El retiro e ingreso de todo activo de información (Equipos de cómputo) de los visitantes que presten servicios a Compañía de Empaques S.A y sus filiales (consultores, pasantes, visitantes, etc.) serán registrado e inspeccionado antes del acceso a las instalaciones de Compañía de Empaques S.A. y sus filiales. El personal asignado en los controles de acceso verificará y registrarán las características de identificación del activo de información.

Cuando ingresan equipos a la empresa serán inventariados por el área de Seguridad Física de la Compañía y si requieren algún acceso a internet, la remoción o ajuste a derechos de accesos a servicios de TI lo solicitará el jefe de área y este será concedido para que acceda a la red de visitantes, la cual no debe tener acceso a ningún recurso de la Empresa.

Creación de cuenta de usuario (Ver Procedimiento para el requerimiento de usuarios y Política de uso de recursos informáticos)

La generación de cuenta de usuario se realiza a través del envío de un correo electrónico por parte del área Desarrollo Organizacional, Talento Humano y jefe Inmediato a TI. Donde se debe indicar que recursos se deben asignar y si requiere equipo, correo electrónico y acceso al ERP

Perfiles de navegación de internet

Se tendrá un único perfil de navegación para los colaboradores, contratistas, terceras partes, que requieran tener acceso a servicios de navegación de internet.

El perfil de navegación de internet relacionado a continuación incluye características de los sitios y servicios web no aprobados por Compañía de Empaques S.A. y sus filiales, no obstante, los sitios deben cumplir con las políticas configuradas en las herramientas de seguridad de la información / ciberseguridad con que cuenta Compañía de Empaques S.A. y sus filiales, por lo cual, aquellos sitios que sean identificados como no confiables, deberán ser bloqueadas por TI.

- Único perfil de navegación en el cual bloquea las siguientes clasificaciones en internet:
- Potencialmente Riesgoso
- Adulto/Contenido para Adulto
- Violación de la Seguridad
- No Categorizado

Cuando se requiera alguna modificación, el usuario enviará un correo a sistemas.Infraestructura@grupoexcala.com autorizado por el jefe inmediato, solicitando el cambio de su perfil de navegación o se adicione la página requerida a las permitidas, para que continue con el mismo perfil de navegación.

Servicio de almacenamiento en redes públicas (Nube - Internet)

Descarga de Archivos: Compañía de Empaques S.A. y sus filiales permitirá a los usuarios, la descarga de archivos desde los sistemas de almacenamiento ubicados en las redes públicas

(Internet), únicamente con fines empresariales, la cual será supervisada con las herramientas de seguridad de la información / ciberseguridad, destinadas para ese fin.

Carga de Archivos: Se niega el acceso a servicios de almacenamiento de información en plataformas públicas, personales o privadas diferentes a la establecidas por Compañía de Empaques S.A y sus filiales, por lo que el uso de otras herramientas como Dropbox, etc., con la finalidad de realizar almacenamiento de información de Compañía de Empaques S.A deberá ser aprobado por el Oficial de Seguridad de la Información o quien haga sus veces.

Acceso remoto

Los colaboradores de Compañía de Empaques S.A. y sus filiales, que requieran realizar conexión remota desde el exterior de las instalaciones de la Compañía en virtud del cargo, cumplimiento de funciones o responsabilidades asignadas, debe realizar la conexión remota a través de una conexión VPN segura configurada por TI.

Todo trabajo por realizarse en las estaciones de trabajo y servidores de Compañía de Empaques S.A. y sus filiales con información de la Empresa, por parte de sus colaboradores, se debe realizar desde la red física de Compañía de Empaques S.A. o sus filiales o de manera remota (VPN Virtual Private Network, "Conexión Privada a la Red") siempre y cuando tenga la aprobación del jefe inmediato.

Acceso a discos de red o carpetas virtuales

El Área de TI tendrá implementado y configurado carpetas virtuales que permitan el almacenamiento de información digital para los usuarios de Compañía de Empaques S.A y de sus filiales, así como las medidas de seguridad que permitan mantener la integridad, disponibilidad e integridad de la información allí almacenada.

Los usuarios que requieran acceso a la información ubicada en las carpetas virtuales, el responsable de la carpeta compartida o el jefe inmediato deberá enviar mediante correo electrónico remitido a sistemas.infraestructura@grupoexcala.com, autorizando el acceso y permisos, correspondientes al rol y funciones a desempeñar. Los usuarios tendrán permisos de escritura, lectura o modificación de información, dependiendo de la solicitud a las funciones y el rol asignado.

PRUEBAS DE SEGURIDAD

Se deberá realizar 1 prueba se seguridad al año, de caja negra con pruebas de ingeniería social. De ser posible que las pruebas incluyan la infraestructura tecnológica y alguna aplicación crítica para el negocio de la Compañía de Empaques S.A. y sus filiales.

El oficial de seguridad o quien haga sus veces, deberá realizar actividades de monitoreo periódico sobre las consultas que se realicen sobre las bases de datos, especialmente las que contengan información personal de terceros (Clientes, proveedores, empleados).

AUDITORÍAS INTERNAS Y EXTERNAS

Se deberá desarrollar un programa de auditoría para verificar el control interno en las personas, proceso y tecnologías enfocadas en la seguridad de la información. (Ver Plan de Auditoría de Seguridad de la Información y Ciberseguridad)

OTRAS DISPOSICIONES

Cualquier modificación de la presente política, será aprobada por el Comité de seguridad de la información y/o La Vicepresidencia Financiera y Administrativa.

ANEXOS

1. Reglamento Interno del Comité de Seguridad de la Información.
2. Procedimiento para identificar, clasificar y conservar los activos de la información.
3. Política interna de Gestión del riesgo.
4. Procedimiento interno de Gestión del riesgo.
5. Procedimiento de respaldo de la información.
6. Procedimiento plan de respaldo contingencias TI.
7. Procedimiento de administración de cámaras.
8. Procedimiento para la seguridad de la información.
9. Procedimiento para el requerimiento de usuarios.
10. Política de uso de recursos informáticos.
11. Procedimiento para Gestión de Incidentes de Seguridad.
12. Clausulado para contrato de Servicios en la Nube.
13. procedimiento de seguridad física.
14. Plan de Auditoría de Seguridad de la Información y Ciberseguridad.