POLÍTICA CORPORATIVA DE CLASIFICACIÓN Y SEGURIDAD EN EL MANEJO DE INFORMACIÓN

1. OBJETIVO

Definir los niveles de clasificación, identificación y etiquetado para la protección de la información de Grupo Carso, a fin de que sea manejada con las medidas de seguridad físicas y lógicas requeridas, por los procesos del negocio, las leyes y regulaciones aplicables en cada caso para proteger su confidencialidad e integridad de los socios, clientes y proveedores.

2. ALCANCE

La presente política es aplicable para todos los colaboradores y personal externo que hagan uso o que tengan acceso a la información digital y sus medios físicos, utilizadas en los procesos de negocio en las empresas que conforman Grupo Carso, S. A. B. de C. V. excepto Grupo Sanborns, S.A.B. de C.V. (LAS EMPRESAS).

3. DEFINICIONES

3.1 Activo de Información. Elemento tangible o intangible, en cualquiera de sus estados y medios de almacenamiento y transferencia, así como la infraestructura tecnológica que la soporta, recibe, envía o genera y que genera valor al utilizarlo para la producción y procesos de negocio, prestación de servicios o para propósitos administrativos.

3.2 Información clasificada: Activos de información que requiere cierto nivel de protección, de acuerdo a los requisitos de confidencialidad definidos por el Propietario de la información, y deben reflejar dicho nivel de protección a través de su respectiva clasificación, en el inventario de activos informáticos,

3.3 Información Secreta. Información altamente sensible que de difundirse puede generar un impacto financiero y/o legal. Activos de información secreta son: Secretos industriales, Datos de ventaja competitiva, Contraseñas, Llaves privadas. Por su naturaleza es de nula divulgación.

3.4 Información Confidencial. Información que requiere acceso limitado a un grupo de colaboradores y en caso de ser robada, puede impactar negativamente las operaciones de LAS EMPRESAS. Por su naturaleza debe ser limitada, incluida aquellos datos que requieren ser protegidos para obligaciones contractuales, financieras y/o legales, cuya utilización indebida podría dar origen a impactos financieros, potencial de fraude o cambios en la posición de mercado de LAS EMPRESAS. Activos de información confidencial son: Cuentas bancarias, estrategias operativas, expedientes de licitaciones, Contratos, Datos personales sensibles, datos protegidos por leyes, datos personales sensibles.

3.5 Información Restringida. Información interna propiedad de LAS EMPRESAS, accesible a todo el personal y no para terceros. Incluyen aquellos datos que son requeridos para el correcto desempeño de las funciones de todos los colaboradores de LAS EMPRESAS para cumplir los objetivos de negocio y niveles de servicio internos establecidos. La utilización indebida puede dar origen a un daño en la operación de una o varias unidades de negocio de LAS EMPRESAS. Activos de información restringida son procedimientos operativos, guías, manuales de operación propietarios de los procesos de las empresas, reglamentos, organigramas.

3.6 Información Pública. Información que puede ser difundida abiertamente, así como toda la información generada internamente por LAS EMPRESAS, cuya justificación de negocio y comercial requiere del uso masivo en medios públicos como es Material de mercadotecnia, Teléfonos de conmutador, Catálogo de productos. Así mismo, información que no es propiedad de LAS EMPRESAS y que fue adquirida por medios públicos y que no tienen restricciones de patente o derechos de autor; fue cedida por terceros para su uso abierto sin cargos o sanciones.

3.7 Propietario de la Información. Director de Sector o Gerente General que reporte de Dirección General de "LAS EMPRESAS" quien define la clasificación, protección y uso de la información de los procesos de negocio bajo su responsabilidad.

3.8 Personal Externo. Proveedores, clientes o terceros, que por necesidades del negocio o que bajo contrato deben desarrollar una actividad o proyecto específico que requiere tener acceso a sistemas, infraestructura tecnológica y/o información de LAS EMPRESAS.

3.9 Medios físicos. Recursos tecnológicos físicos que reflejan o resguardan los activos de información digitales que se transforman o transfieren a un medio de almacenamiento o un medio impreso.

Para definiciones adicionales Consultar Anexo A "Glosario de Términos de Seguridad Informática" de PO-CORP-DF-11Política General de Seguridad Informática.

4. LINEAMIENTOS

4.1. DE LA CLASIFICACIÓN DE LA INFORMACIÓN

4.1.1 Se debe clasificar y etiquetar una vez que la información se genere, obtenga, adquiera o transforme; o se reciba una solicitud de acceso a la misma, aunque no se hubiera clasificado previamente.

4.1.2 Los propietarios de la información son responsables de asegurar que toda la información de los procesos de negocio a su cargo, se clasifique y etiquete durante todo su ciclo de vida que incluye la creación, almacenamiento, transferencia, transporte, modificación, resguardo y en los distintos medios y formatos (electrónico o físico) autorizados, y para ello deberá reflejar dicha clasificación en el inventario de activos de información de la unidad del negocio respectivo.

4.1.3 La clasificación de información debe aplicar tanto a activos de información físicos como digitales de LAS EMPRESAS, así como activos de información externos o generados por otras entidades, pero cuyo acceso y uso es controlado y restringido.

4.2. NIVELES DE CLASIFICACIÓN DE LA INFORMACIÓN

La clasificación y etiquetado a la información y a los medios usados en el ciclo de vida de ésta se deben aplicar de acuerdo con el Procedimiento Corporativo de Clasificación de información.

4.3. DEL ETIQUETADO DE LA INFORMACIÓN

4.3.1 Los propietarios de la información deben señalar aquellos activos de información, incluyendo expedientes y documentos que contengan partes o secciones "Confidenciales" y "Restringidas" que, para ser expuestas en medios públicos, deban omitirse. Asimismo, de ser requerido hacerla pública, debe evaluarse y generarse una versión pública de los expedientes o documentos, y autorizada por el Director de Sector, en caso de recibir una solicitud de dicha información.

4.3.2 La información impresa y/o digital, debe llevar una etiqueta de su clasificación en la superficie de esta. La etiqueta para cada uno de los documentos debe ser fácilmente identificable, visible y suficiente para cumplir su función. La etiqueta de clasificación debe incluirse en las presentaciones de LAS EMPRESAS, y debe mostrarse en por lo menos una de las vistas.

4.3.3 Los medios físicos de información deben ser clasificados, etiquetados y gestionados conforme a la información que procesen o contengan, de manera que siempre hereden la clasificación de información más alta.

4.3.4 La información que no esté etiquetada, por omisión se considerará de nivel "Confidencial" y en caso de que sea requerida una clasificación diferente, el propietario de la información debe establecer es responsable de establecer el criterio de clasificación que le corresponde de acuerdo con el Procedimiento Corporativo de Clasificación de Información.

4.4. DEL INTERCAMBIO DE INFORMACIÓN CON TERCEROS

4.4.1 Ningún colaborador está autorizado a compartir la información clasificada como "Confidencial", sin la autorización de la Dirección del Sector correspondiente y de la Dirección General, o el acuerdo o de confidencialidad estipulado en el punto 4.4.2 de esta política, y debe cumplir con los requerimientos de control y protección definidos para tal efecto en la presente política.

4.4.2 Todo intercambio o transferencia de información con terceros debe estar respaldada por los acuerdos de confidencialidad y de intercambio de información declarados en la parte contractual incluyendo la revisión por el área jurídica y ejecutarse de acuerdo con el "Procedimiento Corporativo de intercambio de información", así como considerar casos en los que aún no se tenga un contrato. los cuales deben contemplar los compromisos adquiridos y las penalizaciones por incumplimiento de dichos acuerdos, así como las cláusulas referentes al manejo, devolución y/o destrucción de información, una vez que el servicio llegue a su término.

4.4.3 Los colaboradores y el personal externo tendrán la responsabilidad de no exponer información de LAS EMPRESAS, Restringida, Confidencial y Secreta, en lugares públicos, absteniéndose por completo de proporcionar a personas ajenas a LAS EMPRESAS, dicha información, salvo en los casos en los que se cuente con autorización de los dueños de la información y en apego al punto 4.4.2 de esta política.

4.5. DE LOS MEDIOS FÍSICOS

4.5.1 Todos los documentos impresos, fotocopiados o escaneados dentro de LAS EMPRESAS, deben ser inmediatamente resguardados a fin de evitar la consulta o uso no autorizado.

Ningún colaborador o tercero dentro de LAS EMPRESAS, debe dejar expuesto en su escritorio o lugar de trabajo, Información COFIDENCIAL o SECRETA impresa, que se encuentre dentro de las instalaciones de LAS EMPRESAS o en el área de trabajo remoto, asegurando que la información sea protegida a través de controles de acceso físico, conforme al nivel de clasificación correspondiente.

4.6 DEL ALMACENAMIENTO Y MANEJO DE LA INFORMACIÓN CLASIFICADA

4.6.1 Se deben implementar controles de acceso físico y lógico para cada nivel de clasificación de información, de acuerdo con los roles, responsabilidades y requisitos de las mejores prácticas de mínimo privilegio "Únicamente lo que se necesita saber".

4.6.2 Toda la información que se refiera a datos personales de un titular debe recopilarse solo después de mostrar una declaración de privacidad y la autorización del propietario de la información conforme los procesos de "Derechos ARCO" que requiere el INAI dentro de su Ley de Protección de Datos Personales en Posesión de Particulares y su Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares correspondiente.

4.6.3 Toda la información clasificada como "Secreta" deberá ser especialmente vigilada por los propietarios de la información y deberán implementarse controles robustos de acceso, autenticación y cifrado.

4.6.4 Si la información clasificada como "Secreta", "Confidencial" o "Restringida" que se contiene en infraestructura de almacenamiento o procesamiento con determinados controles de seguridad, se exporta o cambia de medio de resguardo; éste último deberá protegerse con el mismo nivel de controles que el medio original.

4.6.5 Toda la información clasificada como "Secreta", "Confidencial" o "Restringida", debe gestionarse única y exclusivamente solo por los medios autorizados por LAS EMPRESAS.

4.6.6 El almacenamiento de información estructurado (base de datos) de LAS EMPRESAS debe gestionarse únicamente en la infraestructura autorizada y aprobada por el Gerente General de Sistemas, no está permitido hacer respaldos o uso de ambientes que no cumplan con lo establecido en política PO-CORP-DF-18 Política Corporativa de Gestión de Respaldos.

4.7 DE LOS CONTROLES DE SEGURIDAD MÍNIMOS REQUERIDOS

4.7.1 De acuerdo con su nivel de clasificación de información se debe cumplir con controles mínimos requeridos como se define en procedimiento corporativo de Clasificación de información

5. RESPONSABILIDADES.

5.1 Colaborador de las empresas.

5.1.1 Salvaguardar y proteger los activos de información, a los que cada uno tiene acceso para el desempeño de sus labores dentro de LAS EMPRESAS, ante cualquier amenaza que ponga en riesgo su disponibilidad, integridad y confidencialidad por pérdida, destrucción, alteración o mal uso.

5.2 Todo el personal externo

5.2.1 Cumplir con los lineamientos generales de esta política y proteger la información en los sistemas y redes a los que tienen acceso para procesar, transmitir o almacenar, así como también reportar cualquier mal uso o incumplimiento de esta política

5.3 Propietarios de la información y Gerentes de procesos de negocio

5.3.1 Establecer la clasificación correspondiente a las categorías de datos, documentos, archivos, carpetas, que están dentro de su área de competencia y responsabilidad. En caso de que exista duda sobre el tipo de clasificación que aplica en la información a su cargo, se debe consultar con la Gerencia General de Sistemas.

5.3.2 Requerir el apoyo de la Gerencia General de Sistemas para definir, implementar y mantener los controles de seguridad que son necesarios y requeridos por la presente política, regulaciones aplicables y los requisitos o estándares de seguridad de terceros según corresponda.

5.3.3 Revisar, actualizar y difundir a las partes interesadas la clasificación de la información anualmente, o bien cuando existan cambios significativos en la organización (funcional o tecnológicos) o por requerimientos regulatorios aplicables a LAS EMPRESAS.

5.4 Gerencia General de Sistemas

5.4.1 Luego de la revisión del inventario de activos información y necesidades de cambios significativos de los procesos de negocio, la presenta "PO-CORP-DF-12 Política Corporativa de la Clasificación y Seguridad en el Manejo de la Información" debe reflejar siempre, dichos cambios y revisiones al menos una vez al año.

5.4.2 Apoyar al propietario de la información en caso de que exista duda sobre el tipo de clasificación que aplica en la información a su cargo.

5.5 Dirección de sector

5.5.1 Divulgar, y vigilar el cumplimiento de la presente Política e implementar el ambiente de Control Interno que permita el cumplimiento de esta.

6. REFERENCIAS

PO-CORP-AI-1 Política Corporativa para la Elaboración y Cumplimiento de Políticas y/o Procedimientos.
INST-CORP-AI-01 Instructivo Guía para la Elaboración de Políticas y/o Procedimientos Corporativos.
PO-CORP-DF-11 Política General de Seguridad Informática.
Anexo A "Glosario de Términos de Seguridad Informática" de PO-CORP-DF-11 Política General de Seguridad Informática.
PO-CORP-DF-18 Política Corporativa de Gestión de Respaldos.
Procedimiento Corporativo de Intercambio de Información.

7. CONTROL DE CAMBIOS

1er emisión diciembre 2021.

8. EXCEPCIONES

Esta Política es de aplicación estricta sin excepciones

9. ANEXOS

Sin Anexos.

Elaboró:	Revisó	Revisó	Vo. Bo.:	Autorizó:
Manuel T López Ruiz	Federico Martinez	Evir Robles Rodriguez	Arturo Spínola García	Antonio Gómez García
Jefe De Seguridad informática	Gerente General De Sistemas	Gerente de Auditoria Interna	Director de Finanzas y Administración	Director General de Grupo Carso, S.A.B.