Las partes externas y
la seguridad de la información

En el Sistema de Gestión de Seguridad de la Información SGSI
La seguridad que se puede lograr a través de medios técnicos es limitada y debería ser soportada por procedimientos y gestión adecuados. La identificación sobre ¿cuáles controles deberían estar implementados? requiere una planificación cuidadosa y atención al detalle. Un SGSI exitoso requiere el apoyo de todos los empleados de la organización.

Puede requerir también la participación de las partes interesadas, los proveedores u otras partes externas. También puede ser necesario asesoramiento especializado de partes externas.

En las Políticas para la seguridad de la información
La alta dirección debería definir y aprobar un conjunto de políticas para la seguridad de la información, que deben ser publicadas y comunicadas a los empleados y a las partes externas pertinentes.

Las políticas organizaciones deberían comunicarse a los empleados y a las partes externas pertinentes de forma que sean relevantes, accesible y comprensible para el lector previsto, por ejemplo, en el contexto de una “conciencia de seguridad de la información, educación y programa de formación”

En el teletrabajo
Las organizaciones que permiten las actividades de teletrabajo deberían emitir una política que defina las condiciones y las restricciones para el uso del teletrabajo. Cuando se considere aplicable y sea permitido por la ley, deberían considerarse acuerdos de licencia de software tales que, las organizaciones pueden llegar a tener responsabilidad de la concesión por licenciamiento para el software de clientes en estaciones de trabajo privadas de los empleados o de usuarios de partes externas.

En las condiciones del empleo
Las obligaciones contractuales de los empleados o contratistas deberían reflejar las políticas de seguridad de la información de la organización, además de aclarar y enunciar las responsabilidades del empleado o contratista por el manejo de información recibida de otras organizaciones o partes externas.

En el uso de activos
Los empleados y los usuarios de partes externas que utilizan o tienen acceso a los activos de la organización deberían ser conscientes de los requisitos de seguridad de la información de la organización, otros activos asociados con información y recursos e instalaciones de procesamiento de la información.

Todos los empleados y usuarios de partes externas deberían devolver los activos de la organización que estén en su poder, al finalizar su relación laboral, contrato o acuerdo.

En la información secreta de autenticación
La asignación de información secreta de autenticación debería ser controlada a través de un proceso formal de gestión. El proceso debería incluir el hecho de que la información secreta de autenticación temporal debería proporcionarse a los usuarios de forma segura; debería evitarse el uso de partes externas o mensajes de correo electrónico sin proteger (texto sin cifrar).

Las partes externas y la seguridad de la información

En los derechos de acceso
Los derechos de acceso de todos los empleados y de los usuarios de partes externas a la información y a los recursos de procesamiento de la información deberían ser eliminados al finalizar el empleo, contrato o acuerdo, o ajustados en caso de cambios.

En la seguridad física
Deberían considerarse e implementarse sobre los perímetros de seguridad física, las instalaciones de procesamiento de información gestionadas por la organización deberían separarse físicamente de aquellas gestionadas por partes externas.

Las áreas seguras deberían ser protegidas por medio de controles de entrada apropiados para asegurarse de que el acceso sea permitido solamente a personal autorizado. Debería considerarse el concederse el acceso de manera restringida al personal de soporte de partes externas a las áreas seguras o a las instalaciones sensibles de procesamiento de la información sólo cuando sea requerido; este acceso debería ser autorizado y supervisado.

Los acuerdos para trabajar en áreas seguras incluyen controles para los empleados y los usuarios de partes externas y cubren todas las actividades que tienen lugar en esas áreas.

El equipo, la información o el software no deberían ser llevados fuera del sitio sin autorización previa. Debería considerarse el identificar aquellos empleados y usuarios de partes externas que tengan autoridad para permitir el retiro de activos fuera de los locales de la organización.

El uso de cualquier equipo que almacene o procese información fuera de las instalaciones de la organización, debería ser autorizado por la alta dirección. Esto se aplica a los equipos propiedad de la organización y al equipo de propiedad privada utilizado en nombre de la organización. Deberían considerarse para la protección de los equipos fuera de las instalaciones de la organización, el hecho de que cuando el equipo ubicado fuera de las instalaciones es transferido entre diferentes personas o partes externas, debería mantenerse un registro que defina la cadena de custodia para el equipo, incluyendo como mínimo, los nombres y las organizaciones de aquellos que son responsables del equipo.

En la transferencia de información
Se deberían establecer acuerdos para la transferencia segura de información del negocio entre la organización y partes externas.

En los acuerdos de confidencialidad
Los acuerdos de confidencialidad o de no divulgación deberían incluir el requisito de proteger la información confidencial usando términos que puedan hacerse cumplir legalmente. Los acuerdos de confidencialidad o de no divulgación son aplicables a las partes externas o a los empleados de la organización. Los elementos deberían seleccionarse o incluirse en consideración con la naturaleza de la otra parte y su acceso permisible o el manejo de información confidencial.

En la respuesta a incidentes
Se debería responder a los incidentes de seguridad de la información por medio de un punto de contacto designado y otras personas pertinentes de la organización o partes externas.

Las partes externas y la seguridad de la información

En la protección de los registros

Algunos registros podrían requerir ser almacenados de manera segura tanto para cumplir con requisitos estatutarios, reglamentarios o contractuales, como para soportar actividades esenciales del negocio. Por ejemplo, los registros que puedan requerirse como evidencia para acreditar que la organización opera dentro de las reglas estatutarias o regulatorias, para asegurar una defensa adecuada contra una posible acción civil o penal, o bien para confirmar el estado financiero de la organización respecto a las partes interesadas, partes externas y auditores. La legislación nacional u otras regulaciones podrían establecer el plazo y contenido de los datos para la retención de la información.