SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Previo al empleo
Se busca asegurarse de que los empleados y contratistas entiendan sus responsabilidades, y que sean aptos para los roles para los cuales están siendo considerados.

Investigación
Se debería realizar la verificación de antecedentes de todos los candidatos al empleo de acuerdo con las leyes, regulaciones y normas éticas pertinentes y debería ser proporcional a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos.

La verificación debería tomar en cuenta toda la legislación pertinente sobre privacidad, protección de datos personales y relativa al empleo y, debería, donde sea permitido, incluir lo siguiente:

a) disponibilidad de referencias de carácter satisfactorio, por ejemplo, una de negocios y una personal;

b) una verificación (completa y exacta) del currículum vitae del postulante;

c) confirmación de las calificaciones académicas y profesionales declaradas;

d) verificación independiente de identidad (pasaporte o documento similar);

e) verificaciones más detalladas, tales como verificación de crédito o antecedentes penales.

Cuando una persona es contratada para un rol específico en seguridad de la información, las organizaciones deberían estar seguras que el candidato:

a) tenga las competencias necesarias para desempeñar el rol de seguridad;

b) pueda ser confiable para asumir el rol, especialmente si el rol es crítico para la organización.

Cuando un trabajo, tanto en un nombramiento inicial o en un ascenso, implica que la persona tenga acceso a recursos de procesamiento de información, y, en particular, si está manipulando información confidencial, por ejemplo, información financiera o altamente confidencial, la organización debería también considerar verificaciones adicionales más detalladas.

Los procedimientos deberían definir criterios y limitaciones para revisiones de verificación, por ejemplo, quién es elegible para seleccionar personal, y cómo, cuándo y por qué se han de realizar las revisiones de verificación.

Debería también realizarse un proceso de investigación para contratistas. En estos casos, el acuerdo entre la organización y el contratista debería especificar las responsabilidades para realizar la investigación y los procedimientos de notificación que necesitan seguir si la investigación no ha sido completada o si los resultados ocasionan duda o preocupación.

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Debería recopilarse la información de todos los candidatos a ser considerados para posiciones dentro de la organización y debería manejarse de acuerdo con la legislación apropiada existente en la jurisdicción pertinente. Dependiendo de la legislación aplicable, los candidatos deberían ser informados con antelación sobre las actividades de investigación.

Términos y condiciones del empleo
Los acuerdos contractuales con los empleados y contratistas deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.

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:

a) que todos los empleados y contratistas a los cuales se les da acceso a información confidencial deberían firmar un acuerdo de confidencialidad o de no-divulgación, previamente a ser otorgado el acceso a los recursos de procesamiento de la información;

b) las responsabilidades legales y derechos de los empleados o contratistas, como, por ejemplo, relativas a derecho de propiedad intelectual o legislación de protección de datos;

c) las responsabilidades para la clasificación de información y gestión de activos organizacionales asociados con la información, los recursos de procesamiento de información y los servicios de información manejados por el empleado o contratista;

d) las responsabilidades del empleado o contratista por el manejo de información recibida de otras organizaciones o partes externas;

e) las acciones a ser tomadas si el empleado o contratista hace caso omiso de los requisitos de seguridad de la organización;

Los roles y responsabilidades de seguridad de la información deberían comunicarse a los candidatos al puesto durante el proceso de pre-empleo.

La organización debería asegurarse de que los empleados y contratistas acuerden, los términos y condiciones concernientes a la seguridad de la información, según la naturaleza y extensión de acceso que ellos tendrán a los activos de la organización asociados con los sistemas y servicios de información.

Cuando sea apropiado, las responsabilidades contenidas dentro de los términos y condiciones de empleo deberían continuar por un período definido luego de la finalización del empleo.

Se puede usar un código de conducta para cubrir las responsabilidades de seguridad de la información de los empleados o contratistas referentes a confidencialidad, protección de datos, ética, uso apropiado de los equipos y recursos de la organización, además de prácticas de buena reputación esperadas por la

organización. Una parte externa, con la cual un contratista está asociado, puede ser necesario que ingrese en acuerdos contractuales en nombre de la persona contratada.

Durante el empleo
Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.

Responsabilidades de la dirección
La dirección debería exigir a todos los empleados y contratistas aplicar la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.

Las responsabilidades de la dirección deberían incluir el aseguramiento de que los empleados y contratistas:

a) sean apropiadamente instruidos sobre sus roles y responsabilidades de seguridad de la información antes de que se le otorgue acceso a información confidencial o a sistemas de información;

b) se les proporcionen directrices para hacer constar las expectativas sobre la seguridad de la información de su rol dentro de la organización;

c) sean motivados a cumplir con las políticas de seguridad de la información de la organización;

d) logren un nivel de conciencia sobre la seguridad de la información pertinente a sus roles y responsabilidades dentro de la organización;

e) cumplan con los términos y condiciones del empleo, lo cual incluye la política de seguridad de la información de la organización y métodos apropiados de trabajo;

f) continúen teniendo aptitudes y cualificaciones apropiadas y sean formados de manera regular;

g) estén provistos con un canal de denuncias anónimas para reportar violaciones de políticas o procedimientos de seguridad de la información (“denuncia de irregularidades”).

La dirección debería demostrar el soporte a las políticas, los procedimientos y controles de seguridad de la información, y actuar como un modelo a seguir.
Información adicional

Si los empleados y contratistas no están conscientes de sus responsabilidades de seguridad de la información, pueden causar un daño considerable a la organización. El personal motivado es probable que sea más confiable y ocasione menos incidentes de seguridad de la información.

Una gestión pobre puede causar que el personal se sienta subestimado resultando en un impacto negativo en la seguridad de la información. Por ejemplo, una gestión

pobre puede conducir a negligencias en la seguridad de la información o un potencial mal uso de los activos de la organización.

Toma de conciencia, educación y formación en seguridad de la información
Todos los empleados de la organización, y cuando sea pertinente, los contratistas, deberían recibir educación y formación apropiada sobre toma de conciencia y actualizar periódicamente las políticas y procedimientos de la organización.

Un programa de concientización de seguridad de la información debería tener como objetivo que los empleados, y cuando corresponda, los contratistas sean conscientes de sus responsabilidades en seguridad de la información y los medios por los cuales esas responsabilidades se liberan.

Debería establecerse un programa de concientización de seguridad de la información alineado con las políticas y los procedimientos pertinentes de seguridad de la información de la organización, tomando en cuenta la información de la organización a ser protegida, y los controles que han sido implementados para proteger la información.

El programa de concientización debería incluir una serie de actividades de toma de conciencia, tales como las campañas (por ejemplo," día de seguridad de la información") y los folletos o boletines informativos.

Debería planificarse el programa de concientización tomando en cuenta los roles de los empleados en la organización y, cuando corresponda, las expectativas de concientización de los contratistas por parte de la organización. Las actividades en el calendario de concientización deberían planificarse en el tiempo, preferiblemente con regularidad, para que las actividades sean repetitivas y cubran a los nuevos empleados y contratistas. El programa de concientización también debería actualizarse regularmente de manera que permanezca alineado con las políticas y los procedimientos organizacionales y debería ser construido a partir de las lecciones aprendidas de los incidentes de seguridad de la información.

La formación de concientización debería ser ejecutada según sea requerido por el programa de concientización en seguridad de la información. La formación de concientización puede usar diferentes medios, incluyendo lecciones presenciales, educación a distancia, basado en la web, auto-aprendizaje y otros.
La educación y la formación en seguridad de la información debería abarcar también aspectos generales, tales como:

a) declaración del compromiso de la dirección con la seguridad de la información en toda la organización;

b) la necesidad de familiarizarse y cumplir con las reglas y obligaciones aplicables de seguridad de la información, según se define en las políticas, normas, leyes, reglamentos, contratos y acuerdos;

c) rendición personal de cuentas por las propias acciones y omisiones, y las responsabilidades generales hacia la obtención o protección de la información que pertenece a la organización y a las partes externas;

d) procedimientos básicos de seguridad de la información (tales como la notificación de incidentes de seguridad de la información) y los controles de línea base (tales como la contraseña de seguridad, los controles ante código malicioso y los escritorios limpios);

e) puntos de contacto y recursos para obtener información adicional y consejos sobre los asuntos de seguridad de la información, incluyendo educación y materiales de formación adicionales en seguridad de la información.

La educación y formación en seguridad de la información deberían realizarse periódicamente. La educación y formación inicial se aplica a quienes son transferidos a nuevas posiciones o roles con requisitos sustancialmente diferentes de seguridad de la información, no solo a los nuevos empleados y debería llevarse a cabo antes de que la función llegue a estar activa.

La organización debería desarrollar un programa de educación y formación para lograr que la educación y formación sean eficaces. El programa debería estar alineado con las políticas y los procedimientos pertinentes de seguridad de la información de la organización, tomando en cuenta la información de la organización a ser protegida y los controles que han sido implementados para proteger la información. El programa debería considerar las diferentes formas de educación y formación, por ejemplo, conferencias o auto-estudio.

Al redactar un programa de concientización, es importante no solo centrarse en el “qué” y “cómo”, sino también en el “por qué”. Es importante que los empleados entiendan el objetivo de la seguridad de la información y el impacto potencial, positivo y negativo, de su propio comportamiento en la organización.

La concientización, la educación y la formación pueden ser parte de, o llevarse a cabo en colaboración con otras actividades de formación, por ejemplo, formación en generalidades de TI o en seguridad. Las actividades de concientización, educación y formación deberían ser apropiadas y pertinentes a los roles, las responsabilidades y las habilidades individuales.

Podría llevarse a cabo una evaluación de la comprensión de los empleados al final de un curso de concientización, educación y formación para poner a prueba la transferencia de conocimientos.

Proceso disciplinario

Debería existir un proceso disciplinario formal y comunicado para tomar acciones contra los empleados que hayan cometido una violación a la seguridad de la información.

El proceso disciplinario no debería comenzar sin una verificación previa de que la violación a la seguridad de la información haya ocurrido.

El proceso disciplinario formal debería asegurar un tratamiento correcto y justo para los empleados de los cuales se sospecha que han violado la seguridad de la información. El proceso disciplinario formal debería proveer una respuesta gradual que tome en consideración factores tales como la naturaleza y gravedad de la violación y su impacto en el negocio, si es la primera ofensa o una repetición, si el

violador fue apropiadamente formado, legislación pertinente, contratos del negocio y otros factores que se requieran.

El proceso disciplinario también debería usarse como disuasión para prevenir que los empleados violen las políticas y procedimientos de seguridad de la información organizacionales, y cualquier otra violación de seguridad de la información. Las violaciones deliberadas pueden requerir acciones inmediatas.

El proceso disciplinario también puede convertirse en una motivación o incentivo si las sanciones positivas son definidas por el comportamiento notable en lo que respecta a la seguridad de la información.

Finalización y cambio de empleo

Se busca proteger los intereses de la organización como parte del proceso de finalización o cambio de empleo.

Terminación o cambio de responsabilidades del empleo

Las responsabilidades de seguridad de la información y tareas que siguen vigentes después de la finalización o cambio de las responsabilidades laborales se deberían definir y comunicar al empleado o contratista y se deberían hacer cumplir.

La comunicación de la terminación de responsabilidades, debería incluir los requisitos de seguridad de la información y las responsabilidades legales en curso y, cuando sea apropiado, las responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad y los términos y condiciones de empleo que continúan por un período de tiempo definido luego de la desvinculación del empleado o contratista.

Las responsabilidades y deberes que permanecen válidos después de la finalización de la relación laboral deberían estar contenidos en los términos y condiciones de empleo de los empleados o contratistas.

Los cambios de responsabilidad o empleo deberían ser gestionados de la misma manera como la finalización de las responsabilidades o empleo actual combinadas con la iniciación de la nueva responsabilidad o empleo.

La función de recursos humanos generalmente es responsable por el proceso completo de desvinculación laboral y trabaja junto con el supervisor de la persona que egresa para gestionar los aspectos de seguridad de la información de los procedimientos pertinentes. En el caso de un contratista, provisto a través de una parte externa, este proceso de finalización es llevado a cabo por la parte externa en conformidad con el contrato entre la organización y la parte externa.

Puede ser necesario informar a los empleados, clientes, o contratistas de los cambios en los acuerdos operativos y de personal.