SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

INTRODUCCIÓN Y ANTECEDENTES

- Antes de la contratación

  Una persona nueva a una empresa implica un nuevo acceso a sistemas de información, antes de contratar a una persona se deberán comprobar todos sus antecedentes incluyendo el contenido del currículum, las certificaciones académicas y profesionales, esto para saber si son convenientes para los papeles que ellos desempeñaran, reduciendo así el riesgo de robo de información, fraude o el mal uso de las Instalaciones.

  Se debe estar seguro de las funciones y de las acciones que llevara a cabo el empleado para no cometer errores que puedan afectar a la integridad de la información de la empresa. Para que sea así, deberán recibir la formación, educación, motivación y concienciación necesaria acerca de procedimientos de seguridad y el correcto uso de la información.

- Durante la contratación

  Deben de estar de acuerdo a firmar los términos y condiciones del empleo y de la organización, en el cual se les informara de las responsabilidades de la seguridad de la información. Las responsabilidades dentro de los términos y las condiciones de empleo deben seguir durante un período definido después del final del empleo, donde se deberá de firmar una confidencialidad de no divulgar la información de dicha organización, al igual que la responsabilidad del manejo, clasificación de la información.

  Para ello se deberá llevar acabo un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad.

- Cese o cambio de puesto de trabajo

  Cuando surga un cambio de puesto de trabajo es recomendable sobre todo examinar que accesos necesita revocar en primer lugar cuando un empleado presenta su carta de dimisión. Al igual que también hacer un seguimiento del uso del e-mail por estas personas antes de salir definitivamente de la empresa, por si comienzan a sacar información confidencial.

OBJETIVOS

Los objetivos que se tienen que tomar en cuenta son los siguientes:

- Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen.

- Asegurarse que todo personal están conscientes de las amenazas de seguridad de sus responsabilidades, obligaciones y que están equipados para cumplir con la política de seguridad de organización en el desempeño de sus labores diarias, para reducir el riesgo asociado a los errores humanos.

- Asegurarse de que los empleados y contratistas están en conocimiento y cumplen con sus responsabilidades en seguridad de la información.

- Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

- Proteger los intereses de la organización durante el proceso de cambio o finalización de empleo por parte de empleados y contratistas.

Algunos de los ejemplos que pueden ser:

- Evitar el riesgo, abandonando el proceso o actividad que lo genera cuando el riesgo exceda a los beneficios que nos aporta.
- Traspasar el riesgo a terceros, por ejemplo, mediante cláusulas contractuales o pólizas de seguros.
- Gestionar el riesgo, estableciendo contramedidas que mitiguen o limiten el riesgo, reduciendo la probabilidad de que se materialicen las consecuencias que de éste se puedan derivar.
- Asumir el riesgo, aceptándolo cuando el establecimiento de las contramedidas supere el coste que pueda suponer la materialización del propio riesgo.

CONTROL DE REVISIÓN APLICABLES

Los controles de revisión que se deben llevar acabo en la la seguridad ligada a los Recursos Humanos son los siguientes:

Seguridad en las responsabilidades laborales.	Definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización.
Selección y política personal.	Revisiones de verificación de antecedentes de los candidatos al empleo, contratistas y terceros y en concordancia con las regulaciones, ética y leyes relevantes. (deben ser proporcionales a los requerimientos del negocio).

Seguridad en las responsabilidades laborales.	Definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización.
Supervisión de las obligaciones .	La dirección deberá requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización.
Formación y capacitación en seguridad de la información.	Todos personal de dicha organización deberán de recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales en cuanto a la función de su trabajo.
Cese de responsabilidades.	Responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas y asignadas.
Restricción de activos.	Empleados, contratistas y terceros deberán devolver todos los activos de la organización que estén en su posesión a la finalización de su empleo, contrato o acuerdo.

PUNTOS DE APLICACIÓN

Hay que tener en cuenta los siguientes puntos para la aplicación de seguridad en Recursos Humanos

- **Manual de seguridad:**
  Es el documento que inspira y dirige todo el sistema, determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales del SGSI (Sistema de gestión de la seguridad de la información).

- **Procedimientos:**
  Son documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

- **Instrucciones, checklists y formularios:**
  Serán los documentos que describen cómo se realizan las tareas relacionadas con la seguridad de la información.

INFORMACIÓN Y ELEMENTOS ADICIONAL

Se podrán complementar los documentos con infografías, fuentes de consulta, sistemas o equipo **que pueda servir de apoyo para la implementación, etc**