

MNEMO



ANEXO 7

SEGURIDAD LIGADA A RRHH

Dentro de esta área se localizan los siguientes objetivos y principios, controles y posibles mediciones asociadas:

A6.1, A6.2	Antes del empleo
Objetivo	Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.
Principios	<p>Garantizar que todo el personal es elegible y adecuado para las funciones para las que se le considera y que sigue siendo elegible y adecuado durante su empleo.</p> <p>Asegurarse de que el personal comprende sus responsabilidades en materia de seguridad de la información en relación con las funciones para las que se le considera.</p> <p>Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo.</p> <p>Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deberían seleccionar adecuadamente, especialmente para los trabajos sensibles.</p> <p>Los empleados, contratistas y usuarios de terceras partes de los servicios de procesamiento de la información deberían firmar un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad.</p>
Información	Conjuntamente con RRHH, asegure que se emplea un proceso de verificación de antecedentes proporcional a la

A6.1, A6.2	Antes del empleo
	<p>clasificación de seguridad de aquella información a la que va a acceder el empleado a contratar.</p> <p>Dicho simplemente, el proceso de contratación de un administrador de sistemas IT, debería ser muy diferente del de un administrativo. Haga comprobaciones de procedencia, formación, conocimientos, etc.</p>
Medición	Porcentaje de nuevos empleados o pseudo-empleados (contratistas, consultores, temporales, etc.) Que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar.

A5.4, A6.3, A6.4	Durante el empleo
Objetivo	Asegurar que los empleados, contratistas y terceras partes son conscientes de las amenazas de seguridad, de sus responsabilidades y obligaciones y que están equipados para cumplir con la política de seguridad de la organización en el desempeño de sus labores diarias, para reducir el riesgo asociado a los errores humanos.
Principios	La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización. Garantizar que el personal y las partes interesadas pertinentes conozcan y cumplan sus responsabilidades en materia de seguridad de la información de la información. Garantizar que el personal y otras partes interesadas pertinentes comprendan las consecuencias de la violación

A5.4, A6.3, A6.4	Durante el empleo
	<p>de la política de seguridad de la información, para disuadir y tratar adecuadamente al personal y otras partes interesadas pertinentes que hayan cometido la violación.</p> <p>Se debería definir las responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización.</p> <p>A todos los usuarios empleados, contratistas y terceras personas se les debería proporcionar 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.</p> <p>Se debería establecer un proceso disciplinario normal para gestionar las brechas en seguridad.</p>
Información	<p>La responsabilidad con respecto a la protección de la información no finaliza cuando un empleado se va a casa o abandona la organización. Asegure que esto se documenta claramente en materiales de concienciación, contratos de empleo, etc.</p> <p>Contemple la posibilidad de una revisión anual por RRHH de los contratos junto con los empleados para refrescar las expectativas expuestas en los términos y condiciones de empleo, incluyendo su compromiso con la seguridad de la información.</p>
Medición	Respuesta a las actividades de concienciación en seguridad medidas por (por ejemplo) el número de e-mails y llamadas relativas a iniciativas de concienciación individuales.

A6.5	Al cese de la relación laboral
Objetivo	Proteger los intereses de la organización cuando empleados, contratistas y terceras partes abandonan la organización.
Principios	Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo o contratos. La organización debe comunicar y recordar a los empleados, contratistas y terceras partes que cesen su actividad en la misma, sus responsabilidades relativas a los requisitos de seguridad de la información, así como las responsabilidades legales y, en su caso, las responsabilidades contenidas en cualquier acuerdo de confidencialidad o de no divulgación (véase 6.6) y los términos y condiciones de empleo (véase 6.2).
Información	Las responsabilidades y obligaciones aún vigentes después de la terminación del empleo deben estar contenidas en los términos del contrato que se ha llevado a cabo con el empleado o contratista de los (ver 6.2).
Medición	Porcentaje de identificadores de usuario pertenecientes a personas que han dejado la organización, separados por las categorías de activos (pendientes de desactivación) e inactivos (pendientes de archivo y borrado).