Listado de amenazas y vulnerabilidades en ISO 27001

Las **amenazas y vulnerabilidades en ISO 27001** son tratadas en el capítulo 8 de la norma. Su correcta identificación es un aspecto clave de un sistema de seguridad de la información dentro del **proceso de evaluación de riesgos.** Amenazas y vulnerabilidades en ISO 27001 van de la mano y, por esa razón, se abordan en un mismo capítulo y deben ser consideradas en su conjunto. **Sin embargo, entre unas y otras existe una diferencia que no siempre es muy clara, sobre todo para los neófitos en la materia.**

La diferencia entre amenazas y vulnerabilidades en ISO 27001

Es muy importante diferenciar claramente entre estos dos atributos de un riesgo, porque **la existencia del riesgo, en sí, depende de la coexistencia de una amenaza y una vulnerabilidad.**

Por un lado, las **vulnerabilidades son defectos o debilidades en un activo.** Por el otro, **las amenazas pueden desencadenar o explotar una vulnerabilidad** para comprometer algún aspecto del activo.

Debemos tener en cuenta que **hay muchas amenazas que no tienen absolutamente ninguna relevancia para muchas organizaciones.** Un ejemplo muy claro, aunque poco probable, es una organización que no tiene Internet. Esta puede estar despreocupada por la gran variedad de amenazas basadas en la conectividad a la red; pues se trata de una organización que no está expuesta a esas amenazas.

Pero si la organización se conecta a Internet, debe empezar a preocuparse por esas amenazas. Un punto de conexión es siempre un posible punto de vulnerabilidad y, por lo tanto, un área donde **se pueden requerir controles**. En este sentido, la selección del control depende de la evaluación de la organización sobre la **probabilidad y el impacto potencial** de amenazas específicas y debe centrarse en tratar de reducir el nivel de amenaza o reducir el alcance de la vulnerabilidad.

En definitiva, **las amenazas son externas a los activos de información y las vulnerabilidades suelen ser atributos o aspectos del activo que la amenaza puede explotar**. Si bien las amenazas tienden a ser externas a los activos, no provienen necesariamente de fuera de la organización. De hecho, la mayoría de los incidentes de seguridad de la información de hoy se originan dentro del perímetro de la organización.

El rango de amenazas y vulnerabilidades en ISO 27001 es muy amplio. Por ello, hemos decidido transcribir un listado de amenazas y vulnerabilidades en ISO 27001 de ejemplo, como una forma de apoyo para los profesionales que trabajan hoy en la implementación del sistema de gestión de seguridad de la información en esta tarea de identificación.

Listado de amenazas y vulnerabilidades en ISO 27001

Las amenazas

- Acceso a la red o al sistema de información por personas no autorizadas.
- Amenaza o ataque con bomba.
- Incumplimiento de relaciones contractuales.
- Infracción legal.
- Comprometer información confidencial.
- Ocultar la identidad de un usuario.
- Daño causado por un tercero.
- Daños resultantes de las pruebas de penetración.
- Destrucción de registros.
- Desastre generado por causas humanas.

- Desastre natural, incendio, inundación, rayo.
- Revelación de información.
- Divulgación de contraseñas.
- Malversación y fraude.
- Errores en mantenimiento.
- Fallo de los enlaces de comunicación.
- Falsificación de registros.
- Espionaje industrial.
- Fuga de información.
- Interrupción de procesos de negocio.
- Pérdida de electricidad.
- Pérdida de servicios de apoyo.
- Mal funcionamiento del equipo.
- Código malicioso.
- Uso indebido de los sistemas de información.
- Uso indebido de las herramientas de auditoría.
- Contaminación.
- Errores de software.
- Huelgas o paros.
- Ataques terroristas.

- Hurtos o vandalismo.
- Cambio involuntario de datos en un sistema de información.
- Cambios no autorizados de registros.
- Instalación no autorizada de software.
- Acceso físico no autorizado.
- Uso no autorizado de material con copyright.
- Uso no autorizado de software.
- Error de usuario.

La identificación de amenazas y vulnerabilidades en #ISO27001 es esencial para una gestión de riesgos adecuada. Compartimos una lista. Clic para tuitear

Las vulnerabilidades

- Interfaz de usuario complicada.
- Contraseñas predeterminadas no modificadas.
- Eliminación de medios de almacenamiento sin eliminar datos.
- Sensibilidad del equipo a los cambios de voltaje.
- Sensibilidad del equipo a la humedad, temperatura o contaminantes.
- Inadecuada seguridad del cableado.
- Inadecuada gestión de capacidad del sistema.
- Gestión inadecuada del cambio.
- Clasificación inadecuada de la información.

- Control inadecuado del acceso físico.
- Mantenimiento inadecuado.
- Inadecuada gestión de red.
- Respaldo inapropiado o irregular.
- Inadecuada gestión y protección de contraseñas.
- Protección física no apropiada.
- Reemplazo inadecuado de equipos viejos.
- Falta de formación y conciencia sobre seguridad.
- Inadecuada segregación de funciones.
- Mala segregación de las instalaciones operativas y de prueba.
- Insuficiente supervisión de los empleados y vendedores.
- Especificación incompleta para el desarrollo de software.
- Pruebas de software insuficientes.
- Falta de política de acceso o política de acceso remoto.
- Ausencia de política de escritorio limpio y pantalla clara.
- Falta de control sobre los datos de entrada y salida.
- Falta de documentación interna.
- Carencia o mala implementación de la auditoría interna.
- Falta de políticas para el uso de la criptografía.
- Falta de procedimientos para eliminar los derechos de acceso a la terminación del empleo.

- Desprotección en equipos móviles.
- Falta de redundancia, copia única.
- Ausencia de sistemas de identificación y autenticación.
- No validación de los datos procesados.
- Ubicación vulnerable a inundaciones.
- Mala selección de datos de prueba.
- Copia no controlada de datos.
- Descarga no controlada de Internet.
- Uso incontrolado de sistemas de información.
- Software no documentado.
- Empleados desmotivados.
- Conexiones a red pública desprotegidas.
- Los derechos del usuario no se revisan regularmente.

Diplomado de Seguridad de la Información con la ISO/IEC 27001:2013

Saber identificar las amenazas y vulnerabilidades en ISO 27001 de acuerdo con el contexto de la organización es de obligado conocimiento **para los profesionales en seguridad de la información**. También lo son todos los requisitos de la norma y los controles del Anexo A.

El **Diplomado de Seguridad de la Información con la ISO/IEC 27001:2013** aborda con profundidad estos y otros temas esenciales de ISO 27001. Con él, los alumnos adquieren la

capacidad y las competencias necesarias para **implementar y auditar** un sistema de gestión de seguridad de la información basado en dicho estándar.

Conozca más sobre lo que este diplomado puede enseñarle aquí.