Dominios de seguridad

Los dominios de seguridad que propone esta norma ISO/IEC 27001:2013, se encuentran estructurados de acuerdo a los componentes y elementos más relevantes para el mejoramiento de los activos de información.

En una organización se deben gestionar, entre otros tantos, los activos de información de manera segura y responsable, esto la norma recomienda que se cuente con políticas claras que aseguren el ejercicio de identificación y aseguramiento de dichos activos de la información.

A continuación, le presentamos la estructuración de otros controles y objetivos de seguridad que se deben tener en cuenta en los procesos de cronograma y diseños de estrategias de ciberseguridad de una organización.

1 Dominios de seguridad

El riesgo de que una organización sea afectada por un incidente es permanente. Cada día se presentan nuevas amenazas que pueden interrumpir o dañar los activos de información de la organización, por ello, en la tabla No 4 se presentan algunos controles sugeridos para reducir este tipo de riesgos.

Tabla 4

A12 Seguridad de las operaciones

A.12.1	**Procedimientos operacionales y responsabilidades:** asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
A.12.1.1	Procedimientos de operación documentados.
A.12.1.2	Gestión de cambios.
A.12.1.3	Gestión de capacidad.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.
A.12.2	**Protección contra código malicioso:** asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra código malicioso.
A.12.2.1	Controles contra código malicioso.
A.12.3	**Copias de respaldo:** proteger contra la pérdida de datos.
A.12.3.1	Respaldo de la información.
A.12.4	**Registro y Seguimiento:** registrar eventos y generar evidencia.
A12.4.1	Registro de eventos.
A12.4.2	Protección de la información de registro.
A12.4.3	Registros del administrador y del operador.
A12.4.4	Sincronización de Relojes.
A12.5.	**Control de Software Operacional:** asegurarse de la integridad de los sistemas operacionales.
A12.5.1	Instalación de software en sistemas operativos.
A12.6	**Gestión de la vulnerabilidad técnica:** prevenir el aprovechamiento de las vulnerabilidades técnicas.
A12.6.1	Gestión de las vulnerabilidades técnicas.
A12.6.2	Restricciones sobre la instalación de software.
A.12.7	**Consideraciones sobre auditoria de sistemas de información:** minimizar el impacto de las actividades de auditoria sobre los sistemas operativos.
A12.7.1	Controles de auditoría de sistemas de información.

Fuente: Norma ISO/IEC 27001:2013 – Anexo A

2 Controles de la seguridad en las redes

Otro factor importante hoy en día, es la transmisión e intercambio de información, por ello, en la tabla No. 5, se presentan algunos controles que nos permiten gestionar la seguridad en las redes, así como en el proceso de transferencia e intercambio de información.

Tabla 5

A13 Seguridad de las comunicaciones

A13.1	**Gestión de la seguridad de las redes:** asegurar la protección de la información de las redes, y sus instalaciones de procesamiento de información de soporte.
A13.1.1	Controles de redes.
A13.1.2	Seguridad de los servicios de red.
A13.1.3	Separación en las redes.
A13.2	**Transferencia de información:** mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
A13.2.1	Políticas y procedimientos de transferencia de información.
A13.2.2	Acuerdos sobre transferencia de información.
A13.2.3	Mensajería electrónica.
A13.2.4	Acuerdos de confidencialidad o de no divulgación.

Nota: Norma ISO/IEC 27001:2013 – Anexo A

3 Controles de desarrollo y mantenimiento

Actualmente las organizaciones cuentan con departamentos o grupos encargados de desarrollar y mantener sus propios soluciones. En la tabla No. 6, se muestran controles que deben ser tenidos en cuenta, en este tipo de actividades.

Tabla 6

A14 Adquisición desarrollo y mantenimiento de sistemas

A13.1	**Requisitos de seguridad de los sistemas de información:** asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.
A13.1.1	Análisis y especificación de requisitos de seguridad de la información.
A13.1.2	Seguridad de servicios de las aplicaciones en redes públicas.
A13.1.3	Protección de transacciones de los servicios de las aplicaciones.
A14.2	**Seguridad en los procesos de desarrollo y de soporte:** asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
A14.2.1	Política de desarrollo seguro.
A14.2.2	Procedimiento de control de cambios en sistemas.
A14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.
A14.2.4	Restricciones en los cambios a los paquetes de software.
A14.2.5.	Principios de construcción de los sistemas seguros.
A14.2.6.	Ambiente de desarrollo seguro.
A14.2.7	Desarrollo contratado externamente.
A14.2.8	Pruebas de seguridad de Sistemas.
A.14.2.9	Prueba de aceptación de Sistemas.
A14.3	**Datos de prueba:** asegurar la protección de los datos usados para prueba.
A14.3.1	Protección de datos de prueba.

Nota: Norma ISO/IEC 27001:2013 – Anexo A

4 Controles para relación con proveedores

La relación con los proveedores de productos o servicios para la organización, debe estar alineado con las políticas de seguridad y, para este caso, la tabla presenta los controles sugeridos que aseguraran un apropiado intercambio de información entre las partes.

Tabla 7

A15 Relaciones con los proveedores

A15.1	**Seguridad de la información en las relaciones con los proveedores:** asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
A15.1.1	Política de seguridad de la información para las relaciones con proveedores.
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores.
A15.1.3	Cadena de suministro de tecnología de información y comunicación.
A15.2.	**Gestión de la prestación de servicios de proveedores:** mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
A15.2.1	Seguimiento y revisión de los servicios de los proveedores.
A15.2.2	Gestión de cambios en los servicios de los proveedores.

Fuente: Norma ISO/IEC 27001:2013 – Anexo A

5 Controles de la gestión de incidentes

Cualquier organización está sujeta a sufrir algún incidente de seguridad que afecte el desarrollo de sus funciones. Reconozca los controles para gestionar este tipo de incidentes y recuperarse lo más rápido posible.

Tabla 8

A16 Gestión de incidentes de seguridad de la información

A16.1	**Gestión de incidentes y mejoras en la seguridad de la información:** asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
A16.1.1	Responsabilidades y procedimientos.
A16.1.2	Reporte de eventos de seguridad de la información.
A16.1.3	Reporte de debilidades de seguridad de la información.
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.
A16.1.5	Respuesta a incidentes de seguridad de la información.
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.
A16.1.7	Recolección de evidencia.

Nota: Norma ISO/IEC 27001:2013 – Anexo A

6 Controles de la gestión de la continuidad

Garantizar la continuidad del negocio es un factor importante tras sufrir un incidente, por ello se presentan en la tabla 9, los controles que garantizan que la organización pueda recuperarse, en un mínimo tiempo, con una mínima pérdida posible de información.

Tabla 9

A17 Aspectos de seguridad de la información de la gestión de continuidad de negocio

A17.1	**Continuidad de seguridad de la información:** la continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad del negocio de la organización.
A17.1.1	Planificación de la continuidad de la seguridad de la información.
A17.1.2	Implementación de la continuidad de la seguridad de la información.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
A17.2	**Redundancias:** asegurar la disponibilidad de instalaciones de procesamiento de información.
A17.2.1	Disponibilidad de instalaciones de procesamiento de información.

Nota: Norma ISO/IEC 27001:2013 – Anexo A

7 Controles del cumplimiento

Finalmente, el cumplimiento de los requisitos legales garantiza el buen actuar de la organización y evita incurrir en alguna falta que afecte, en un futuro a la organización. Identifique, en la tabla, los controles que buscan reducir los riesgos, al incurrir en una falta relacionada.

Tabla 10

A18 Cumplimiento

A18.1	**Cumplimiento de requisitos legales y contractuales:** evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.
A18.1.2	Derechos de propiedad intelectual.
A18.1.3	Protección de registros.
A18.1.4	Privacidad y Protección de información de datos personales.
A18.1.5	Reglamentación de controles criptográficos.
A18.2	**Revisiones de seguridad de la información:** asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
A18.2.1	Revisión independiente de la seguridad de la información.
A18.2.2	Cumplimiento con las políticas y normas de seguridad.
A18.2.3	Revisión del cumplimiento técnico.

Nota: Norma ISO/IEC 27001:2013 – Anexo A

Estos objetivos de control, pueden ser estudiados con mayor profundidad, consultando directamente en la norma **ISO/IEC 27001:2013 – Anexo A**. Allí usted podrá identificar aspectos más relevantes sobre este punto.