**¿Qué es un estándar?**

Un estándar es un conjunto de reglas, normas o directrices que se establecen para lograr un nivel de uniformidad, calidad o compatibilidad en un determinado contexto. Los estándares son creados y adoptados por organizaciones o entidades con el propósito de establecer un marco común que asegure la consistencia, la interoperabilidad y la confiabilidad en diferentes campos.

Un ejemplo común de estándar en la tecnología es el estándar IEEE802.11, que se refiere a las especificaciones para redes inalámbricas Wi-Fi.

En la industria automotriz, el estándar ISO 9001 establece requisitos para os sistemas de gestión de calidad.

Y así sucesivamente, en cada una de las áreas se cuentan con estándares que permiten controlar la calidad de un producto y así garantizar que al momento de que se sigan, se esta adquiriendo/comprando un producto de excelente producción.

Algunas organizaciones más importantes sobre estandarización se encuentran:

**ISO:** Organización Internacional de Normalización: desarrolla estándares internacionales en una amplia variedad de campos.

**IEEE** Instituto de Ingenieros Eléctricos y Electrónicos: crea estándares en áreas como tecnología de la información, electrónica y telecomunicaciones.

**NIST** Instituto Nacional de Estándares y Tecnología: en los estados unidos, desarrolla estándares en tecnología y seguridad.

**ANSI** Instituto Nacional Estadounidense de Estándares: coordinador de normas voluntarias en los EUA.

**Objetivo:**

Es reducir los riesgos, incluida la prevención o mitigación de los ciberataques. Estos materiales publicados consisten en colecciones de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, pautas, enfoques de gestión de riesgos, acciones, capacitación, mejores prácticas, aseguramiento y tecnologías.

**Familia ISO/27000**

La familia de normas ISO 27000 se refiere a una serie de estándares internacionales relacionados con la gestión de la seguridad de la información. Estos estándares son desarrollados por la **Organización Internacional de Normalización (ISO)** y se centran en proporcionar un marco de trabajo para establecer, implementar, mantener y mejorar un **sistema de seguridad de la información (SGSI).**

La serie de normas ISO 27000 incluye varios estándares, siendo los más conocidos:

ISO 27001 – Sistema de Gestión de Seguridad de la Información (SGSI)

ISO 27002 – Código de Practica para Controles de Seguridad de la Información

ISO 27005 – Gestión de Riesgos de Seguridad de la Información

ISO 27003 – Guía de Implementación del SGSI

ISO 27017 Y ISO 27018 – Guías para la Seguridad en la Nube

Otras categorías dentro de la familia 27000 se encuentran:

|  |  |
| --- | --- |
| **Vocabulario común** | ISO 27000 |
| **Requisitos** | ISO 27001, ISO 27006, ISO 27009 |
| **Guías de aplicación** | ISO 27002, ISO 27003, ISO 27004, ISO 27005, ISO 27007, TR ISO 27008  ISO 27013, ISO 27014, ISO 27015, TR 27016, ISO 27021 |
| **Requisitos específicos** | ISO 27010, ISO 27011, ISO 27017, ISO 27018, ISO 27019 |

**Incidente de seguridad**

Un incidente de seguridad se refiere a un evento no deseado o a una serie de eventos que comprometen la integridad, confidencialidad o la disponibilidad de los sistemas de información, datos o recursos de una organización.

Algunos incidentes de seguridad pueden incluir:

* Brechas de datos
* Ataques cibernéticos
* Perdida de dispositivos/datos
* Accesos no autorizados
* Fugas de información
* Abuso de privilegios

**Desastre**

Es un evento no planificado que inhabilita el centro de datos de la organización, lo que evita que se pueda operar de forma normal. Un peligro, combinado con vulnerabilidad e incapacidad para reducir sus consecuencias negativas potenciales da lugar a un desastre.

**Actividades de gestión de accidentes**

1. **DETECCIÓN**

* Identificar la presencia de un incidente o accidente. Esto puede implicar el monitoreo continuo de sistemas, la vigilancia de procesos o la observación de eventos inusuales.
* Establecer sistemas de recolección de eventos que nos permitan monitorear las alertas de seguridad.

1. **CLASIFICACIÓN**

* Evaluar la gravedad del incidente o accidente sirve para determinar su impacto en la seguridad y la operación de la organización. Esto puede incluir la asignación de niveles de severidad.
* Analizar los incidentes de seguridad que se hayan detectado, documentarlos y catalogarlos estableciendo su prioridad.
* Estudiar los incidentes que hayan tenido lugar analizando sus causas, y así poder establecer mediad de seguridad adicionales que protejan nuevos activos de nuevos incidentes de índole similar.

1. **NOTIFICACIÓN**

* Informar a las partes relevantes sobre el incidente o accidente. Esto puede incluir la notificación a las autoridades pertinentes, a los equipos de respuesta de emergencia o a los responsables dentro de la organización.
* Poner en marcha un punto central de comunicación, para recibir y difundir información de incidentes de seguridad entre las partes correspondientes.

1. **RESPUESTA INMEDIATA**

* Tomar medidas rápidas para contener el incidente o accidente y mitigar cualquier daño adicional. Esto puede incluir la activación de planes de respuesta de emergencia y la movilización de recursos.
* Establecer procedimientos de respuesta ante incidentes y mantenerlos actualizados para saber que pasos debemos dar y así gestionarlos correctamente.

1. **INVESTIGACIÓN**

* Llevar a cabo una investigación detallada para determinar las causas subyacentes del incidente o accidente. Esto implica recopilar evidencia, entrevistar testigos y analizar datos.

1. **DOCUMENTACIÓN**

* Registrar los detalles relevantes del incidente o accidente. Esto es esencial para futuros informes, seguimiento y lecciones aprendidas.

1. **COMUNICACIÓN**

* Mantener a todas las partes interesadas informadas sobre el estado de la situación, las acciones tomadas y los próximos pasos. Esto incluye la comunicación interna y externa.

1. **RECUPERACIÓN**

* Restaurar la operación normal tan pronto como sea posible después del incidente o accidente. Esto puede implicar la restauración de sistemas, la recuperación de datos y reparación de los daños.

1. **LECCIONES APRENDIDAS**

* Evaluar el incidente o accidente para identificar las áreas de mejora en los procesos, procedimientos o políticas de seguridad. Estas lecciones ayudan a prevenir incidentes similares den el futuro.

1. **INFORME Y NOTIFICACIÓN**

* Cumplir con los requisitos legales y relacionados con la notificación de incidentes o accidentes, especialmente en industrias altamente reguladas.

1. **ENTRENAMIENTO Y CAPACITACIÓN**

* Proporcionar capacitación continua al personal sobre como prevenir incidentes y como responder adecuadamente en caso de que ocurran

1. **EVALUACIÓN DE RIESGOS**

* Identificar y evaluar los riesgos asociados con incidentes y accidentes para implementar medidas preventivas.

**Plan de contingencia y continuidad de negocio**

Las empresas deben estar preparadas para prevenir, protegerse, y reaccionar antes incidentes de seguridad que pueden afectarles y que podrían impactar en sus negocios.

Existen 3 tipos según su alcance o ámbito que tengan:

* Plan de recuperación ante desastres
* Plan de continuidad TIC
* Plan de continuidad de negocio

**Plan de recuperación antes desastres (DRP)**

Es un documento detallado que establece las estrategias y los procedimientos que una organización debe seguir para recuperar sus sistemas de información y operaciones criticas después de un desastre o incidente grave. El objetivo principal de un DRP es garantizar la continuidad del negocio y minimizar el impacto de los desastres en la organización.

**Evento de seguridad:**

* Respuesta
* Notificación
* Evaluación del daño
* Declaración
* Recuperación
* Operaciones en contingencia
* Restauración

**El documento debe contener:**

* Alcance y objetivos
* Equipo de recuperación
* Evaluación de riesgos
* Procedimientos de recuperación
* Copia de seguridad
* Infraestructura de respaldo
* Recuperación de comunicación y aplicaciones
* Recursos humanos
* Comunicación y coordinación
* Pruebas y mantenimiento
* Formación y concienciación
* Auditoría

Un plan de continuidad de negocios es un conjunto de procedimientos y estrategias diseñada para garantizar que una organización pueda continuar operando de manera eficiente en caso de interrupciones, desastres o incidentes que puedan afectar el funcionamiento normal. El BCP es una parte integral de la gestión de riesgos y la planificación estratégica de una organización.

Planes de contingencia

Una propuesta para el desarrollo y aplicación del DRP se considera en los siguientes 6 puntos:

1. Desarrollar una política de continuidad
2. Realizar una evaluación de riesgos
3. Realzar análisis de impacto de negocio (BIA)
4. Desarrollar estrategias de recuperación y continuidad del negocio
5. Concientizar, capacitar y probar planes
6. Mantener y mejorar el plan de recuperación ante desastres

**Tecnologías de respuesta ante los incidentes**

Existen muchas tecnologías que se utilizan para implementar una respuesta ante los incidentes:

* **Comisión de admisión de redes (NAC):** permite el acceso a la red para los usuarios autorizados con sistemas compatibles. Un sistema compatible cumple con todos los requisitos de las políticas de la organización.
* **Los sistemas de detección de intrusos (IDSs):** supervisan de forma pasiva el trafico en la red. Los sistemas IDS son pasivos.
* **Los sistemas de prevención de intrusos:** funcionan en el modo en línea. Puede detectar y abordar inmediatamente un problema de red.
* **NetFlow e IPFIX:** NetFlow es una tecnología de Cisco que proporciona estadísticas sobre los paquetes que atraviesan un router o un switch de multicapa.

**La inteligencia de amenazas avanzadas:**

**Consideración de la continuidad de los negocios:** los controles de la continuidad de los negocios no solo realizan una copia de respaldo de los datos y proporcionan el hardware redundante. Las consideraciones de la continuidad de los negocios deben incluir:

* Documentar las configuraciones
* Establecer canales de comunicación alternativos
* Proporcionar energía
* Identificar todas las dependencias para las aplicaciones y los procesos
* Comprender como realizar las tareas automatizadas manualmente

**Mejores prácticas de la continuidad de los negocios:**

1. Escriba una política que proporcione orientación para desarrollar un plan de continuidad de los negocios y asigne roles para realizar tareas.
2. Identifique los sistemas y los procesos críticos, y priorícelos según la necesidad.
3. Identifique las vulnerabilidades, las amenazas y calcule los riesgos.
4. Identifique e implemente controles y contramedidas para reducir el riesgo.
5. Elija los métodos para recuperar los sistemas críticos rápidamente
6. Escriba procedimientos

**ANALISIS DE RIESGOS DE SEGURIDAD**

**Riesgos de seguridad**

Un riesgo de seguridad se refiere a la posibilidad de que ocurra un evento o incidente que tenga un impacto negativo en la seguridad de la información, los activos de una organización o la integridad de sus sistemas y operaciones.

Estos riesgos pueden manifestarse de diversas maneras y pueden ser causados por una variedad de factores, incluyendo amenazas externas e internas, vulnerabilidades en sistemas y procesos, y la falta de medidas de seguridad adecuadas.

**Análisis de riesgos informáticos**

Es la evaluación de distintos peligros que afectan a nivel informático y que pueden producir situaciones de amenaza al negocio, como robos o intrusiones que comprometan los datos o ataques externos que impidan el funcionamiento de los sistemas propiciando periodos de inactividad empresarial.

**Administración de riesgos**

Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

* Inspección física
* Levantamiento del mapa de riesgos general de la empresa
* Análisis especializados de acuerdo con la actividad desarrollada
* Elaboración del informe con las recomendaciones incluyendo cronograma de implementación de soluciones y valor estimado de la inversión
* Control y seguimiento a la recomendaciones o mejoras implementadas

**Evaluación de riesgos**

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas de la información y a las instalaciones de procesamiento de esta, la probabilidad de que ocurran y su potencial impacto en la operativa de la UNC.

**Ventajas de análisis de riesgos informáticos**

**Identificación de amenazas y vulnerabilidades:** el análisis de riesgos permite a las organizaciones identificar las amenazas potenciales y las vulnerabilidades en sus sistemas y redes. Esto ayuda a comprender donde pueden producirse ataques o incidentes de seguridad.

**Priorización de recursos:** al evaluar y cuantificar los riesgos, las organizaciones pueden priorizar sus recursos y esfuerzos de seguridad. Pueden enfocarse en abordar las áreas de mayor riesgo, lo que permite un uso más eficiente de los recursos.

**Reducción de costos:**

**Mejora de planificación de seguridad:**

**Cumplimiento regulatorio:**

**Mejora de la toma de decisiones:**

**Concientización del personal:**

**Mejora continua:** el análisis de riesgos es un proceso continuo. A medida que la tecnología y las amenazas evolucionan, las organizaciones pueden seguir evaluando y actualizando sus estrategias de seguridad.

**Factores para los riesgos de seguridad**

* Ausencia de un respaldo seguro de datos
* Usuarios mal informados
* Poca inversión

**Gestión de riesgos**

La gestión de riesgos es un proceso integral que se utiliza en diversas áreas y contextos, desde los negocios hasta la seguridad, para identificar, evaluar, controlar y mitigar los riesgos potenciales que podrían afectar los objetivos de una organización. La gestión de riesgos es esencial para tomar decisiones informadas y estratégicas, minimizar pérdida y asegurar la continuidad del negocio.

El objetivo de gestión de riesgos es que la empresa establezca un nivel de tolerancia a cada riesgo.

**Etapas de la gestión de riesgos**

* Identificación de riesgos
* Evaluación de riesgos
* Priorización
* Desarrollo de técnicas de mitigación
* Implementación de controles
* Monitoreo
* Comunicación y concientización
* Documentación
* Mejora continua