HACKER MENTOR

ACADEMIA DE CIBERSEGURIDAD

GLOSARIO

Términos Básicos Relacionados a la Norma ISO 27001

ACADEMIA DE CIBERSEGURIDAD

GLOSARIO

TÉRMINOS BÁSICOS RELACIONADOS A LA NORMA ISO27001

A

ACCESO:

Proceso por el cual un usuario puede ingresar a un sistema de información y realizar acciones.

ACTIVIDAD:

Cualquier acción realizada por un usuario en un sistema de información.

AMENAZA:

Evento que puede explotar una vulnerabilidad en un sistema de información y causar un daño.

ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA):

Evaluación independiente de los controles de seguridad de la información dentro de una organización.

ANÁLISIS DE RIESGOS:

Evaluación de los riesgos potenciales para la seguridad de la información y su probabilidad de ocurrencia.

AUDITORÍA EXTERNA:

Evaluación independiente de los controles de seguridad de la información de una organización realizada por una entidad externa.

AUDITORÍA INTERNA:

Evaluación del impacto que un incidente de seguridad de la información tendría en el negocio de la organización.

AUTENTICACIÓN Y CONTROL DE ACCESO:

Medidas de seguridad para asegurar que solo los usuarios autorizados tengan acceso a la información y los sistemas de la organización.

AUTORIZACIÓN:

Proceso por el cual se otorga permiso a un usuario para acceder a un recurso o realizar una acción.

B

BACKUP:

Copia de seguridad de la información para su restauración en caso de pérdida o daño.

C

CAPACITACIÓN Y CONCIENCIA:

Proceso para capacitar a los empleados sobre las políticas y procedimientos de seguridad de la información y para aumentar su conciencia sobre la importancia de la seguridad de la información.

CONTINUIDAD DEL NEGOCIO:

Planes y procedimientos para garantizar que la organización pueda continuar operando en caso de interrupción del negocio.

CONTROL DE ACCESO:

Procedimientos para garantizar que solo los usuarios autorizados puedan acceder a la información.

CONTROL DE ACCESO LÓGICO:

Medidas de seguridad para controlar el acceso a los sistemas y la información de la organización a través de controles de acceso basados en roles, contraseñas, autenticación multifactorial, entre otros.

CONTROL DE ACCESO FÍSICO:

Medidas de seguridad para controlar el acceso a los edificios y las áreas físicas de la organización mediante controles de acceso físico como tarjetas de acceso, cámaras de seguridad, entre otros.

CONTROL DE CAMBIOS:

Proceso para gestionar los cambios en los sistemas y la información de la organización para garantizar que los cambios sean apropiados y no afecten negativamente la seguridad de la información.

CRIPTOGRAFÍA:

Medidas de seguridad para proteger la información mediante la utilización de técnicas de cifrado.

CUMPLIMIENTO LEGAL Y CONTRACTUAL:

Proceso para asegurar que la organización cumple con los requisitos legales y contractuales relacionados con la seguridad de la información.

E

EVALUACIÓN DE LA CONFORMIDAD:

Proceso de revisión de los controles de seguridad de la información para garantizar que cumplan con los requisitos de la norma ISO 27001.

EVALUACIÓN DE RIESGOS:

Proceso para identificar, analizar y evaluar los riesgos para la seguridad de la información de la organización, y para determinar las medidas de seguridad adecuadas para mitigar o reducir estos riesgos.

EVALUACIÓN DE TERCEROS:

Proceso de evaluación de la seguridad de los proveedores y otros terceros que tienen acceso a la información de la organización.

EVALUACIÓN Y MEJORA CONTINUA DEL SGSI:

Proceso para evaluar y mejorar continuamente el sistema de gestión de la seguridad de la información de la organización para garantizar la protección efectiva de la información.

EVALUACIÓN Y SELECCIÓN DE PROVEEDORES:

Proceso para evaluar y seleccionar proveedores de servicios y productos que cumplan con los requisitos de seguridad de la información de la organización.

G

GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD:

Proceso para detectar, investigar y responder a incidentes de ciberseguridad.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:

Proceso para detectar, investigar y responder a incidentes de seguridad de la información.

GESTIÓN DE LA PRIVACIDAD DE LA INFORMACIÓN:

Proceso para proteger la privacidad de la información personal de los individuos, incluyendo su recolección, uso, almacenamiento y divulgación.

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EXTERNALIZACIÓN:

Proceso para garantizar que los servicios de externalización contratados por la organización cumplan con los requisitos de seguridad de la información establecidos por la organización.

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA VIRTUALIZACIÓN:

Proceso para garantizar que los sistemas virtualizados de la organización cumplan con los requisitos de seguridad de la información.

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN PROYECTOS:

Proceso para integrar la gestión de la seguridad de la información en proyectos de la organización.

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO:

Procesos y procedimientos para garantizar que la organización pueda continuar operando en caso de interrupción del negocio.

GESTIÓN DE LA SEGURIDAD LÓGICA:

Medidas de seguridad para proteger los sistemas y la información de la organización, como la autenticación y la protección de datos.

GESTIÓN DE LA SEGURIDAD FÍSICA:

Medidas de seguridad para proteger los activos físicos de la organización, como los edificios y equipos.

GESTIÓN DE ACTIVOS:

Proceso de gestión de los activos de información de la organización, incluyendo su propiedad, clasificación y valoración.

GESTIÓN DE CAMBIOS:

Proceso de gestión de los cambios en los sistemas y procesos de la organización para garantizar que se realicen de manera segura y controlada.

GESTIÓN DE CONTRASEÑAS:

Procesos para establecer, gestionar y controlar las contraseñas de los usuarios para garantizar que sean seguras y que se utilicen correctamente.

GESTIÓN DE DOCUMENTOS:

Proceso para controlar y gestionar los documentos relacionados con la seguridad de la información de la organización, incluyendo su creación, revisión, aprobación y distribución.

Recurso Gratuito Hacker Mentor
2023 Glosario Términos Básicos relacionados a la Norma ISO27001

GESTIÓN DE INCIDENTES:

Procedimientos y medidas implementados para detectar, responder y recuperarse de los incidentes de seguridad de la información.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:

Procedimientos para detectar, investigar y responder a incidentes de seguridad de la información.

GESTIÓN DE PARCHES:

Proceso para aplicar parches de seguridad y actualizaciones de software para proteger los sistemas y la información de la organización.

GESTIÓN DE PROVEEDORES:

Proceso para asegurar que los proveedores de la organización cumplan con los requisitos de seguridad de la información establecidos por la organización.

GESTIÓN DE VULNERABILIDADES:

Proceso para identificar, evaluar y tratar las vulnerabilidades en los sistemas y procesos de la organización.

GESTIÓN EN LA CADENA DE SUMINISTRO:

Proceso para garantizar que los proveedores y terceros involucrados en la cadena de suministro de la organización cumplan con los requisitos de seguridad de la información establecidos por la organización.

INCIDENTE DE SEGURIDAD:

Cualquier evento que pueda poner en peligro la seguridad de la información de la organización.

M

MANTENIMIENTO Y MEJORA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN:

Proceso para asegurar que el sistema de gestión de la seguridad de la información de la organización se mantenga actualizado y mejore continuamente para garantizar la protección efectiva de la información de la organización.

MEJORA CONTINUA:

Proceso mediante el cual una organización busca mejorar continuamente su sistema de gestión de seguridad de la información.

MEJORAS DE SEGURIDAD:

Procedimientos y medidas para mejorar la seguridad de la información de la organización.

MONITOREO Y REGISTRO DE ACTIVIDADES:

Medidas para monitorear y registrar las actividades de los usuarios en los sistemas de la organización con el fin de detectar posibles actividades maliciosas o inapropiadas.

MONITORIZACIÓN Y REVISIÓN:

Proceso para supervisar y revisar el sistema de gestión de seguridad de la información de la organización para garantizar que siga siendo efectivo y adecuado.

P

PLAN DE CONTINUIDAD DEL NEGOCIO (BCP):

Documento que establece los procedimientos que se deben seguir para garantizar la continuidad del negocio en caso de un incidente de seguridad de la información.

PLAN DE RESPUESTA A INCIDENTES:

Documento que establece los procedimientos que se deben seguir en caso de un incidente de seguridad de la información.

PLAN DE TRATAMIENTO DE RIESGOS:

Documento que describe las medidas de seguridad específicas que se tomarán para mitigar o reducir los riesgos identificados durante el proceso de evaluación de riesgos.

POLÍTICA DE GESTIÓN DE CONTRASEÑAS:

Documento que establece los requisitos y las medidas para la gestión de las contraseñas de los usuarios de la organización.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (PSI):

Documento que establece los objetivos y principios de seguridad de la información de la organización.

POLÍTICA DE SEGURIDAD DE TERCEROS:

Documento que establece los requisitos de seguridad que los terceros deben cumplir para trabajar con la organización.

PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA:

Medidas de seguridad para proteger la información clasificada de la organización.

PROTECCIÓN CONTRA SOFTWARE MALICIOSO:

Medidas de seguridad para proteger los sistemas y la información de la organización contra el software malicioso, incluyendo virus, gusanos, troyanos, entre otros.

PROTECCIÓN DE LA INFORMACIÓN EN DISPOSITIVOS MÓVILES:

Medidas de seguridad para proteger la información de la organización en dispositivos móviles, incluyendo teléfonos inteligentes, tabletas y laptops.

PRUEBAS DE SEGURIDAD:

Proceso para evaluar la seguridad de los sistemas y la información de la organización mediante la realización de pruebas de penetración, escaneos de vulnerabilidades, pruebas de seguridad de aplicaciones, entre otras.

PRUEBA Y REVISIÓN:

Proceso de prueba y revisión de los controles de seguridad de la información para garantizar que sigan siendo efectivos y adecuados para proteger la información de la organización.

PRUEBAS DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRES:

Proceso para evaluar la efectividad del plan de continuidad del negocio y recuperación ante desastres de la organización mediante la realización de pruebas regulares.

S

SEGURIDAD DE LA INFORMACIÓN

Medidas de seguridad para proteger la información de la organización, incluyendo su confidencialidad, integridad y disponibilidad.

SEGURIDAD DE LA RED:

Medidas de seguridad para proteger los sistemas y la información de la organización en redes y comunicaciones.

SEGURIDAD EN LA NUBE:

Medidas de seguridad para proteger los sistemas y la información de la organización que se encuentran en la nube.

SEGURIDAD EN DISPOSITIVOS MÓVILES:

Medidas de seguridad para proteger los dispositivos móviles de la organización y la información que contienen.

SEGURIDAD EN LA GESTIÓN DE LOS ACTIVOS:

Medidas de seguridad para proteger los activos de la organización, incluyendo los activos de la información y los activos físicos.

SEGURIDAD EN LAS COMUNICACIONES:

Medidas de seguridad para proteger las comunicaciones de la organización, incluyendo el correo electrónico, la mensajería instantánea y las comunicaciones de voz.

SEGURIDAD FÍSICA:

Medidas de seguridad para proteger los activos físicos de la organización.

SEGURIDAD LÓGICA:

Medidas de seguridad para proteger los activos lógicos de la organización, como la información almacenada en sistemas informáticos.

T

TERCEROS:

Entidades que proporcionan servicios a la organización y que pueden tener acceso a la información de la organización.

TRATAMIENTO DE RIESGOS:

Acciones tomadas para reducir, transferir, aceptar o evitar riesgos de seguridad de la información.

ACADEMIA DE CIBERSEGURIDAD

REFERENCIAS

TÉRMINOS BÁSICOS RELACIONADOS A LA NORMA ISO27001

NORMA ISO27001

Documento de la Norma ISO27001

HACKER MENTOR