Términos y Definiciones

Aceptación del riesgo

Decision de asumir un riesgo.[Guía ISO/IEC 73:2002]

Activo

Cualquier cosa que tiene valor para la organización. [NTC 5411-1:2006]

Activo de información

Datos o información que se almacena en cualquier tipo de medio y que es considerada como sensitiva o crítica. [Universidad Distrital de Caldas]

Administracion Riesgos

Proceso de identificación, control y reducción 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. [Universidad Distrital de Caldas]

Amenazas

Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización [ISO/IEC 13335-1:2004]

Análisis de Riesgo

Uso sistemático de la información para identificar las fuentes y estimar el riesgo. [Guía ISO/IEC 73:2002]

Auditabilidad

Define que todos los eventos de un sistema deben poder ser registrados para su control posterior. [Gobierno en línea]

Autenticidad

Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información. validando el emisor para evitar suplantación de identidades. [Gobierno en línea]

Cadena de Custodia

En el ámbito de la seguridad de la información La cadena de custodia es la aplicación de una serie de normas y procedimientos tendientes a asegurar, depositar y proteger cada activo de información para evitar la pérdida de integridad, disponibilidad o confidencialidad. [Universidad Distrital de Caldas]

Comunicación del Riesgo

Intercambiar o compartir la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas. [ISO/IEC Guía 73:2002]

Confidencialidad

Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. [NTC 5411-1:2006]

Control

Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

NOTA. El control también se utiliza como sinónimo de salvaguarda o contramedida

Declaración de Aplicabilidad

Documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.

Disponibilidad

Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006]

Estimación Cualitativa

La estimación cualitativa utiliza una escala de atributos calificativos para describir la magnitud de las consecuencias potenciales (por ejemplo, alta, intermedia y baja) y la probabilidad de que ocurran dichas consecuencias. [NTC/ISO 27005:2005]

Estimación Cuantitativa

La estimación cuantitativa utiliza una escala con valores numéricos (a diferencia de las escalas descriptivas utilizadas en la estimación cualitativa) tanto para las consecuencias como para la probabilidad.

Estimación del Riesgo

Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo. [ISO/IEC Guía 73:2002]

NOTA 1. En el contexto de esta norma, el término "actividad" se utiliza en lugar del término "proceso" para la estimación del riesgo.

NOTA 2. En el contexto de esta norma, el término "posibilidad" se utiliza en lugar del término "probabilidad" para la estimación del riesgo.

Evaluación del Riesgo

Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. [Guía ISO/IEC 73:2002]

Evento de Seguridad de la Información

Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [ISO/IEC TR 18044:2004]

Evitación del Riesgo

Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Gestión del Riesgo

Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. [Guía ISO/IEC 73:2002]

Hacker

Es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar. [Gobierno en línea]

Identificación del Riesgo

Proceso para encontrar, enumerar y caracterizar los elementos de riesgo. [ISO/IEC Guía 73:2002]

NOTA En el contexto de esta norma, el término "actividad" se utiliza en lugar del término "proceso" para la identificación del riesgo.

Impacto

Cambio adverso en el nivel de los objetivos del negocio logrados.

Información

Toda comunicación o representación de conocimiento, como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea digital, en papel, en pantallas de computadoras, audiovisual u otro. [Gobierno en línea]

Incidente de Seguridad de la información

Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC TR 18044:2004]

Integridad

Propiedad de salvaguardar la exactitud y estado completo de los activos. [NTC 5411-1:2006]

Legalidad

Referido al cumplimiento de las leyes, normas, reglamentaciones, disposiciones a las que está sujeto la entidad. [Gobierno en línea]

Lineamiento

Una descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas [ISO/IEC 13335-1:2004]

Medios de Procesamiento de la Información

Cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.

No repudio

Evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió. [Gobierno en línea]

Phishing

Es un delito cibernético con el que por medio del envío de correos se engaña a las personas invitándolas a que visiten páginas web falsas de entidades bancarias o comerciales. Allí se solicita que verifique o actualice sus datos con el fin de robarle sus nombres de usuarios, claves personales y demás información confidencial. [Gobierno en línea]

Política

Intención y dirección general expresada formalmente por la gerencia x.

Propietarios de Activos de Información
En el contexto de la norma NTC 27001, un propietario de activos de información es cualquier persona o entidad a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos. [Universidad Distrital de Caldas]

Protección a la Duplicación
Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original. [Gobierno en línea]

Reducción del Riesgo
Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo. [ISO/IEC Guía 73:2002]

NOTA En el contexto de esta norma, el término "posibilidad" se utiliza en lugar del término "probabilidad" para la reducción del riesgo.

Retención del Riesgo
Aceptación de la pérdida o ganancia proveniente de un riesgo particular. [ISO/IEC Guía 73:2002]

NOTA En el contexto de los riesgos en la seguridad de la información, únicamente se consideran las consecuencias negativas (pérdidas) para la retención del riesgo.

Riesgo

Combinación de la probabilidad de un evento y su ocurrencia [ISO/IEC Guía 73:2002]

Riesgo en la Seguridad de la Información

Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

NOTA: Se mide en términos de una combinación de la probabilidad de que suceda un evento y sus consecuencias.

Riesgo Residual

Nivel restante de riesgo después del tratamiento del riesgo. [Guía ISO/IEC 73:2002]

Seguridad de la Información

Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*Accountability*), no repudio y fiabilidad. [NTC-ISO/IEC 17799:2006]

Sistema de Información

Conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. [Gobierno en línea]

Sistema de Gestión de la Seguridad de la Información (SGSI)

Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Smishing

Es una variante del Phishing, pero a diferencia de este, usa mensajes de texto para engañar a los usuarios, pidiéndoles información privada e invitándolos a que se dirijan a sitios web falsos que tienen spywares y softwares maliciosos que se descargan automáticamente, sin que el usuario lo note. [Gobierno en línea]

Tecnología de la Información

Se refiere al hardware y software operado por la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo. [Gobierno en línea]

Transferencia del Riesgo
Compartir con otra de las partes la pérdida o la ganancia de un riesgo. [ISO/IEC Guía 73:2002]

NOTA En el contexto de los riesgos en la seguridad de la información, únicamente se consideran las consecuencias negativas (pérdidas) para la transferencia del riesgo.

Tratamiento del Riesgo

Proceso de selección e implementación de medidas para modificar el riesgo. [Guía ISO/IEC 73:2002]

Valoración del Riesgo

Proceso global de análisis y evaluación del riesgo. [Guía ISO/IEC 73:2002]

Vishing

Similar al Phishing, pero con teléfonos. Consiste en hacer llamadas telefónicas a las víctimas, en las que por medio de una voz computarizada, muy similar a las utilizadas por los bancos, se solicita verificar algunos datos personales e información bancaria. [Gobierno en línea]

Vulnerabilidad
La debilidad de un activo o grupo de activos que puede ser explotada por una o más

amenazas. (ISO/IEC 13335-1:2004)

Fuente: http://www2.utp.edu.co/gestioncalidad/sin-categoria/277/terminos-y-definiciones