**Seguridad informática**

Seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional todo lo relacionado con esta y especialmente la información conectada o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (BBDD, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo siesta información llega a manos de otra persona.

La seguridad de la información no debe ser confundida con la seguridad informática ya que esta última solo se encarga de la seguridad en el medio informático. Pero la información puede encontrarse en diferentes medios o formas y no solo en medios informáticos

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos, y técnicas destinadas a conseguir un sistema seguro y confiable.

**Otra definición de seguridad informática**

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Un sistema informático puede ser protegido desde un punto de vista Lógico (con el desarrollo de software) o Físico (vinculado al mantenimiento eléctrico)

**RTO**

A fin de estar preparados para una eventualidad, los especialistas recomiendan determinar de antemano dos valores: el **objetivo de tiempo de recuperación** y el **objetivo de punto de recuperación**, mejor conocidos por las siglas **RTO y RPO**, respectivamente.

Aunque ambos términos se complementan, también existen diferencias entre RTO y RPO, las cuales explicaremos más adelante. Primero conoce más sobre cada uno a continuación.

el Tiempo Objetivo de recuperación (RTO) es el tiempo hasta el que una empresa puede volver a la normalidad tras el fallo de un servidor o destrucción del sitio donde alberga los equipos informáticos o sea es el tiempo que pasará antes que una infraestructura esté disponible.

Los negocios que dependen de los sistemas informáticos tienen un tiempo de repuesta limitada para recuperarse de un desastre sin poner su estabilidad en juego. Esa ventana, que puede equivaler a minutos, días u horas, es lo que se conoce como objetivo de tiempo de recuperación

Los expertos en seguridad en TI recomiendan diseñar un plan de contingencia acorde con este valor. Hacer esto, te permitirá definir de antemano el presupuesto, el personal y las medidas a seguir para reponerse de una falla crítica dentro del plazo establecido.

**RPO**

Punto objetivo de recuperación (RPO) se refiere al volumen de datos en riesgo de pérdida que la organización considera tolerable. Una falla en una aplicación o en una pieza crítica de hardware podría ocasionar una pérdida de datos. A fin de minimizar las consecuencias, los departamentos de soporte técnico de muchas empresas realizan [copias de seguridad](https://blog.apser.es/2017/09/28/5-motivos-los-una-copia-seguridad-tus-sistemas/) de forma regular. El RPO es el **tiempo que tiene que transcurrir entre la pérdida de la información y la última copia de seguridad**.

Un buen objetivo de punto de recuperación es aquel que no minimiza ni sobrestima la necesidad de hacer una copia de seguridad. Cuando el cálculo es correcto, la compañía no desperdicia tiempo y recursos, ni tampoco corre riesgos innecesarios.

El RPO determina el objetivo de posible pérdida máxima de datos introducidos desde el último backup, hasta la caída del sistema, y no depende del tiempo de recuperación

**BIA**

Conocido como análisis de impacto de negocios (BIA) tiene por objeto analizar los impactos a los que la organización puede enfrentarse ante la discontinuidad de sus operaciones, así como las dependencias de las tecnologías y los sistemas informáticos corporativos.

**Sus objetivos**: El BIA permitirá a su organización identificar para cada proceso o actividad el impacto que tendría la interrupción, el período de tiempo máximo después de una interrupción dentro del cual tiene que continuarse la operación, El nivel mínimo al que la actividad tiene que ser ejecutada cuando se recupera, El periodo máximo de tiempo antes que los niveles normales de operación tengan que haberse recuperado.

**Beneficios:** se delimitan los procesos o actividades críticas dentro de la organización que afectan nuestro negocio pudiendo descubrir actividades que a priori no lo parecían, permite identificar vulnerabilidades de una organización en materia de continuidad de negocio, en caso de disponer de planes de recuperación permitirá verificar si estos cubren las necesidades del negocio, propicia la implicación de un mayor número de áreas de la organización a la hora de implantar planes de continuidad, no solo al personal responsable de llevar a término este tipo de proyectos, reducción de costes ante posibles interrupciones del negocio, aporta información de gran valor a la hora de priorizar el desarrollo de otros proyectos en materia de continuidad de negocio, Un mayor conocimiento de los procesos de negocio, contribuirá favorablemente a la mejora de la competitividad y seguridad en el mercado, la información obtenida en el desarrollo del BIA es una base fundamental para implantar estrategias de recuperación eficientes.

**¿porque realizar un análisis de impacto?**

Todas las empresas están expuestas a sufrir incidentes o eventos no deseados que pueden generar múltiples consecuencias negativas para una organización. Pueden, por ejemplo, paralizar la productividad, generar pérdidas económicas, crear una mala reputación empresarial o hacer que la organización pierda información sensible y confidencial. Por tanto, tener identificadas las amenazas más evidentes a los que se enfrenta la organización y el impacto que tendrían en el que caso de que se materializaran es fundamental para minimizar los riesgos y actuar frente a ellos.

**ALE**

Un paradigma en la seguridad de la información es el concepto de expectativa de pérdida anual (ALE), que permite modelar el impacto que los riesgos de seguridad pueden tener sobre los activos de una organización. Es un elemento que puede ser utilizado durante la realización de [análisis de riesgos](https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/) o directamente en un análisis de costo-beneficio para destinar [recursos al área de seguridad de la información.](https://www.welivesecurity.com/la-es/tag/rosi/) Es un elemento que puede ser utilizado durante la realización de [análisis de riesgos](https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/) o directamente en un análisis de costo-beneficio para destinar [recursos al área de seguridad de la información.](https://www.welivesecurity.com/la-es/tag/rosi/)

ALE es una fórmula algebraica que multiplica el valor de un evento discreto de pérdida (**expectativa de pérdida individual** o SLE) por su **expectativa anual de ocurrencia** (ARO), es decir, la pérdida monetaria que se puede esperar para un activo debido a la materialización de una o más amenazas en un periodo de un año. Se define a través de la siguiente formula: ALE= SLE x ARO

SLE=FE x VA

* **ALE:** Expectativa de Pérdida Anual
* **SLE:** Expectativa de Pérdida Individual
* **ARO:** Tasa de Ocurrencia Anualizada
* **FE:** Factor de Exposición
* **VA:** Valor del activo

Las principales desventajas de ALE recaen en la**ausencia de información** para estimar la probabilidad de ocurrencia o de pérdidas, es decir, la dificultad para generar datos estadísticos que permitan tener un mayor apego al impacto y probabilidad de los riesgos.

**ROSI**

ROSI o Retorno de la Inversión en Seguridad de la Información, por sus siglas en inglés, es un concepto utilizado a nivel de gestión de la seguridad de la información para justificar la implementación de controles que mitigan riesgos tecnológicos o cibernéticos. Hoy en día, con el crecimiento y fortaleza de las APT (Amenazas Avanzadas Persistentes, por sus siglas en inglés), los responsables de la seguridad de la información en las organizaciones, requieren demostrar ante la alta dirección la necesidad de tratar los riesgos que estas amenazas generan y el lenguaje a utilizar, el cual es el mismo que hablan los financieros, es el del dinero. En este sentido, el ROSI, el cual se expresa en dinero, no puede faltar en ninguna presentación de un proyecto de seguridad. Tradicionalmente, para cualquier gestor una inversión debe tener unos ingresos superiores a la misma, de lo contrario no es viable.

**¿Cómo cuantificar o medir entonces la rentabilidad de la seguridad?**

El problema es que, si bien podemos calcular el coste total de la inversión en Seguridad de la Información, los ingresos los deberíamos medir como el ahorro de costes ante un incidente en nuestros sistemas. Pero la opinión general en las empresas y de algunos profesionales de nuestro país es que es difícil de calcular y cuantificar. Sin embargo, hay una manera de estimar los beneficios financieros (es decir, ahorro de costes) de seguridad de la información y de cuantificar la inseguridad.

En primer lugar, es necesario estimar el coste del daño potencial que se produciría ante un incidente, teniendo en cuenta los siguientes factores:

**\*El alcance del incidente potencial, qué departamentos se verían afectados, unidades y procesos del negocio.**

**\*El coste externo de la reposición de equipos, bienes y materiales que fueron dañados por el siniestro.**

**\*El coste interno de los empleados dedicados a resolver el incidente.**

**\*Sanciones legales y/o contractuales si no se cumple con la legislación vigente o con nuestros clientes.**

**\*La pérdida de ingresos, tanto de los clientes actuales, como de los potenciales en el momento del siniestro.**

El siguiente paso consiste en estimar la probabilidad del suceso**.** Para ello hay que tener en cuenta las amenazas y vulnerabilidades de nuestro actual sistema, así como las medidas de seguridad existentes en el momento de la evaluación. La mejor manera es evaluar la frecuencia temporal con la que un incidente de este tipo podría tener lugar.  Cuando se multiplica la esperanza de pérdida y la probabilidad del suceso, obtenemos la Esperanza Perdida Anualizada (**ALE**).

Por último, es necesario estimar cuánto va a costar las medidas de seguridad a implantar teniendo en cuenta los siguientes factores:

**\*Valor de adquisición. Coste del hardware, del software, servicios de implementación, etc…**

**\*Valor residual de las medidas de seguridad.**

**\*Los costes externos de mantenimiento.**

**\*Los costes internos de mantenimiento, principalmente empleados destinados al efecto.**

Cuando tengamos todos estos gastos en conjunto, sabremos si el Retorno de Inversión en Seguridad es positivo o no (la disminución en el riesgo tiene que ser mayor que el coste total de las medidas de seguridad*)* es decir, que el cálculo de las posibles pérdidas anualizadas tiene que ser mayor que el coste anual de las medidas de seguridad adoptadas.