MÓDULO 4

PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

Prof. Mg. Rafael Mellado S.
rafael.mellado@pucv.cl
COM5163 – Sistemas de Información 3
Escuela de Comercio

PRESENTACIÓN DEL MÓDULO

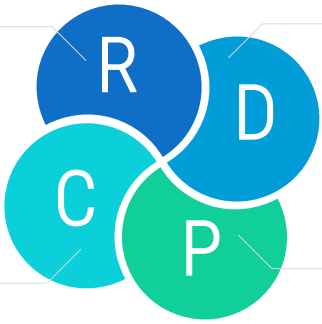
- Errores comunes en las empresas de generalizar a los activos de la empresa como activos tangibles.
- Existen bienes intangibles como cartera de clientes, conocimiento comercial, propiedad intelectual, entre otros.
- Existen empresas que basan su negocio en tratamiento de información.
- Un error es pensar que una empresa por ser pequeña no necesita protección de la información.

PROBLEMA PRINCIPAL

- Tecnologías de procesamiento de grandes volúmenes de datos han potenciado el almacenamiento y uso de la información en la empresa.
- El tratamiento y gestión de la información es poco controlada generando riesgos.
- Las empresas no saben manejar ni tienen políticas para el tratamiento de la información de carácter confidencial.

ERRORES TRATANDO LA INFORMACIÓN

Respaldos
No se cuenta con respaldos de seguridad de la información importante a la empresa.



Dispositivos
Ingreso de hardware a la empresa que no ha sido autorizado y menos controlado.

Control
Se comparten recursos sin control de acceso, ni versionamiento, ni control de cambios.

Política
No existen políticas para dar de baja recursos de hardware ni software.

DIMENSIONES DE LA SEGURIDAD DE LA INFORMACIÓN

Disponibilidad
La información debe estar disponible cuando la empresa la necesite.

Integridad
La información debe ser correcta y estar libre de modificaciones y errores.

Confidencialidad
La información debe ser accesible únicamente por el personal autorizado.

DIMENSIONES DE LA SEGURIDAD DE LA INFORMACIÓN

- Las dimensiones mencionadas anteriormente son los pilares fundamentales para la seguridad de la información.
- La evaluación de los activos de información de la empresa en relación a las dimensiones determina la dirección en la integración de medidas y controles.
- Implantar controles para potenciar una dimensión puede afectar negativamente otra.

SELECCIÓN DE SALVAGUARDAS

- Las salvaguardas son las medidas necesarias para proteger la información.
- Se deben considerar los siguientes aspectos:
  - Determinar la importancia de la información que se maneja en la empresa.
  - Identificar, clasificar y valorar la información según las dimensiones de seguridad para posteriormente seleccionar salvaguardas.
  - Conocer la naturaleza de los controles que se pueden implantar.
  - Consideración de costos de las medidas a implementar.

SELECCIÓN DE SALVAGUARDAS

- La importancia de la información para la empresa depende del sector del mercado en que se trabaje. Se debe considerar:

Sanitario

Grandes volúmenes de información de pacientes.

Financiero

Información confidencial de clientes como de operaciones financieras.

Industrial

Confidencialidad de procesos y procedimientos productivos que generan ventajas competitivas.

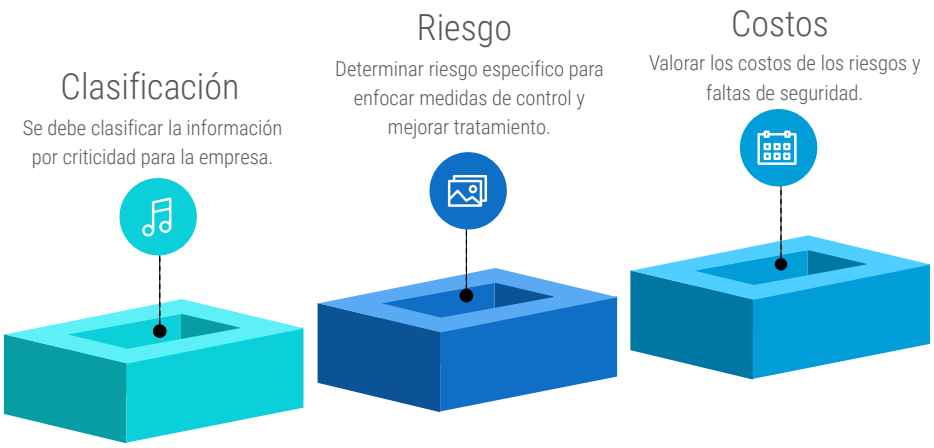
Hotelería

Manejo de datos personales y de reservas que puede afectar la confidencialidad.

SELECCIÓN DE SALVAGUARDAS

- Tipos de datos personales:
  - Los que revelan ideologías, afiliaciones sindicales, opiniones políticas o creencias religiosas.
  - Los que revelan origen racial o étnico y relativos a la salud o vida sexual, genéticos o biométricos.
  - Datos de condenas penales o administrativas.

SELECCIÓN DE SALVAGUARDAS: consideraciones previas



SELECCIÓN DE SALVAGUARDAS: pasos previos

Conocer la información que gestiona la empresa.

Clasificar la información según criticidad.

Determinar el grado de seguridad.

Establecer medidas necesarias para mejorar seguridad.

SELECCIÓN DE SALVAGUARDAS

- Un elemento relevante es conocer la naturaleza de los controles:
  - Técnica
  - Organizativa
  - Física
- También se puede considerar otro tipo de control relacionados a la legalidad vigente en la República.

CRITERIOS DE SELECCIÓN DE SALVAGUARDAS

- Costo de implantación de la medida de seguridad:
  - Costo económico de la medida.
  - Costo en tiempo y recursos humanos.
  - Costo de las posibles medidas alternativas.
  - Costos de las pérdidas económicas que supondría no tener implantada la medida.

→

CRITERIOS DE SELECCIÓN DE SALVAGUARDAS

- La necesidad de cada sistema de información:
  - Determinar qué dimensión de seguridad es más importante proteger (confidencialidad, integridad o disponibilidad).
- La importancia de cada sistema de información en la empresa:
  - Identificar activos más críticos y necesarios de proteger.
  - Contemplar las particularidades de cada sector del negocio.

SALVAGUARDAS BÁSICAS

- Existe un gran número de salvaguardas, definidas en múltiples estándares y normativas internacionales.
- Algunas de estas normativas, como la ISO 27002, son de carácter general, mientras que otras cubren ámbitos y propósitos específicos.
- Las medidas de seguridad a aplicar dependerán del tipo de sistemas a proteger, de la información que contienen, de las condiciones particulares de cada instalación y de las amenazas a las que se exponen.

CONTROL DE ACCESO A LA INFORMACIÓN

- Se debe priorizar respetar el principio del mínimo privilegio:
  - Un usuario sólo debe tener acceso a aquella información estrictamente necesaria para desempeñar sus funciones.
- Para conseguir este objetivo, previo a la implementación de medidas técnicas o salvaguardas, se debe realizar una serie de pasos:
  - Definir tipos de información que existen en la empresa, ej: datos de recursos humanos, contables, clientes, marketing, producción, etc.

→

CONTROL DE ACCESO A LA INFORMACIÓN

- Establecer políticas de acceso a cada tipo de información. Se recomienda realizar una matriz que cruce información con áreas o departamentos que tienen necesidad de acceso a dicha información: →

CONTROL DE ACCESO A LA INFORMACIÓN

		PERFILES DE LA ORGANIZACIÓN				
		PERSONAL DIRECTIVO	PERSONAL DE ADMINISTRACIÓN	PERSONAL DE INFORMÁTICA	PERSONAL OPERARIO	PERSONAL DE ATENCIÓN AL CLIENTE
APLICACIONES DE LA ORGANIZACIÓN	EMAIL	SI	SI	SI	SI	SI
	REMUNERACIONES	NO	SI	NO	NO	NO
	CLIENTES	SI	SI	NO	NO	SI
	FACTURACIÓN	SI	SI	NO	NO	NO
	PAGINA WEB	NO	NO	SI	NO	NO
	SERVIDORES	SI	SI	SI	NO	SI
	PEDIDOS	SI	SI	NO	SI	SI
	INVENTARIO	NO	NO	NO	SI	NO

CONTROL DE ACCESO A LA INFORMACIÓN

- Establecer políticas de acceso a cada tipo de información. Se recomienda realizar una matriz que cruce información con áreas o departamentos que tienen necesidad de acceso a dicha información. ←
- Establecer quién y cómo debe autorizar el acceso a los diferentes tipos de información. Se debe tener trazabilidad sobre procesos que conceden acceso y control de la información.

CONTROL DE ACCESO A LA INFORMACIÓN

- Se debe establecer mecanismos para revisar periódicamente que los permisos concedidos son adecuados:
  - Comprobar con periodicidad la correcta asignación de los permisos.
  - Prestar especial atención a los servicios accesibles desde el exterior, como el uso del correo electrónico corporativo desde fuera de la empresa o el acceso de usuarios a nuestra infraestructura a través de VPN.
- No limitarse al control de acceso lógico e incluir, cuando sea necesario, controles de acceso físico.

COPIAS DE SEGURIDAD

- Las copias de seguridad son la salvaguarda básica para proteger la información.
- Dependiendo del tamaño y necesidades de la empresa, los soportes, la frecuencia y los procedimientos para realizar las copias de seguridad pueden ser distintos.

COPIAS DE SEGURIDAD: soportes

COPIAS DE SEGURIDAD

- Para la implantación de un sistema de copias se debe tener en cuenta:
  - Analizar la información que se va a copiar, así como los sistemas y repositorios donde se encuentra.
  - Configutaciones de dispositivos de red, los equipos de los usuarios o incluso información en smartphones.
  - Se debe descartar información sin relación directa con el negocio o archivos históricos de los que ya existen copias.
  - Definir formalmente el número de versiones que se van a almacenar de cada elemento, y su periodo de conservación.

COPIAS DE SEGURIDAD

- Deben hacerse pruebas de restauración periódicas. Esto es especialmente importante si no se solicitan restauraciones con frecuencia.
- Debe llevarse un inventario de los soportes de copia, mediante un etiquetado y un registro de la ubicación de los soportes.
- Si la información almacenada es confidencial se debe cifrar, para evitar que ante una pérdida o sustracción de un soporte, sea posible acceder a ésta.
- Se debe disponer de una copia de seguridad fuera de la organización, para evitar la pérdida de la información en caso de incendio, inundación, robo o ser víctima de un malware que rastree nuestra red buscando estas copias de seguridad.

COPIAS DE SEGURIDAD

- Se debe documentar el proceso de realización y restauración de copias.
- En caso de que se utilice almacenamiento cloud para las copias de seguridad, se debe considerar la posibilidad de que no se pueda acceder a la información de manera temporal, por un fallo del servicio o de nuestra conexión a Internet.

Copia total: se realiza una copia completa y exacta de la información original.

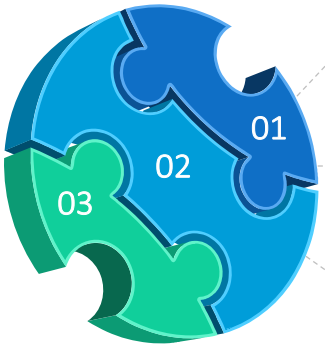
Sistemas de copia incremental: únicamente se copian los archivos que se hayan añadido o modificado desde la última copia realizada.

Sistema de copias diferenciales: cada vez que se realiza una copia de seguridad, se copian todos los archivos que hayan sido modificados.

CIFRADO DE INFORMACIÓN

- Consiste en ofuscar la información mediante técnicas de codificación, evitando que los datos sean legibles por cualquier persona que desconozca la clave de decodificación:
  - Permiten controlar el acceso a la información.
  - Limitan la difusión no autorizada en caso de pérdida o robo de soportes.

CIFRADO DE INFORMACIÓN



La clave debe ser robusta para dificultar el acceso no autorizado a la información.

La pérdida de la clave de acceso imposibilita el acceso a la información.

Cuando ocurre un error físico no es posible la recuperación de la información.

CIFRADO DE INFORMACIÓN

- Programas habituales como las suites de ofimática o compresores de ficheros incorporan funcionalidades de cifrado para proteger la información.
- La elección de la herramienta de cifrado dependerá de:
  - Si se quiere una herramienta transparente al usuario o no.
  - Si el descifrado de la información debe realizarse en cualquier lugar.
  - El perfil del usuario que va a utilizar la herramienta de cifrado.

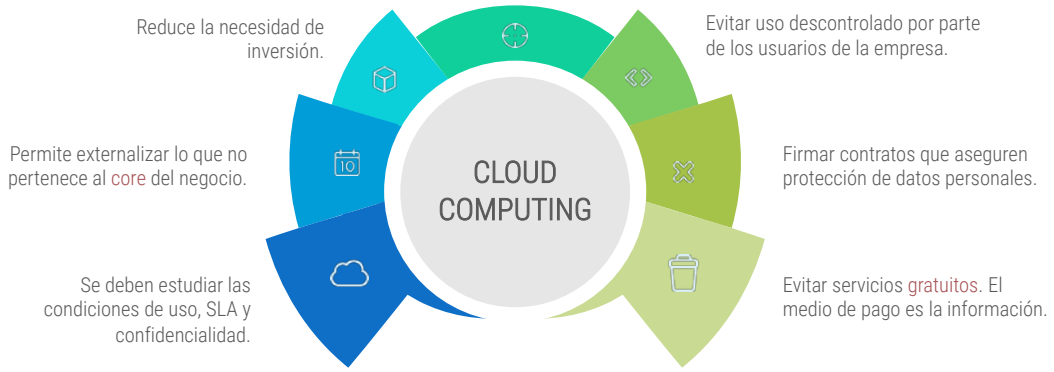
BAJA DE ACTIVOS DE HARDWARE

- Antes de eliminar o reutilizar hardware que haya almacenado información corporativa se deben aplicar las medidas de seguridad necesarias para evitar la recuperación de la información que previamente contuvieron.
- A la hora de valorar los soportes de información, también se debe tener en cuenta la información que se almacena en papel, que se suele desechar sin las adecuadas medidas de seguridad.

BAJA DE ACTIVOS DE HARDWARE

- Existen dos medidas básicas en relación con la información que almacene el soporte, según su destino:
  - Si se va a reutilizar, vender, regalar o prestar, se debe realizar un borrado seguro del soporte.
  - Si se va a desechar el soporte, se debe garantizar que nadie puede utilizarlo posteriormente, y que la información que contiene no puede ser recuperada.
- Sea cual sea la opción escogida, siempre el auditor se debe asegurar que no será posible recuperar la información.

ALMACENAMIENTO CLOUD



CONFIDENCIALIDAD EN CONTRATACIÓN

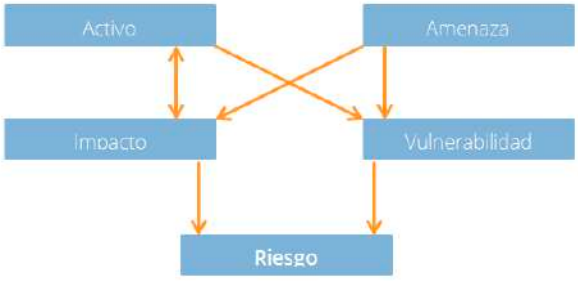
- Todos los servicios de la empresa se pueden tercerizar:
  - Creación de las copias de seguridad, almacenamiento en la nube, destrucción física de soportes, mantenimiento informático, etc.
- La externalización puede introducir nuevos riesgos para la seguridad de la información, derivados del acceso del proveedor a los datos.
- Una medida que mitiga (pero no elimina) este tipo de riesgo es la firma de contratos de confidencialidad o inclusión de este tipo de cláusulas en el contrato de servicio.

CONFIDENCIALIDAD EN CONTRATACIÓN

- Esto compromete al prestador del servicio a no hacer un uso fraudulento de los datos, y adquiere especial relevancia si se externaliza la gestión de datos de carácter personal ya que este acuerdo es un requisito legal obligatorio.

ISO 27001

- Los activos son necesarios para que la empresa funcione y consiga los objetivos que se ha propuesto la alta dirección.
- Los activos se encuentran relacionados, directa o indirectamente, con:



ISO 27001: características de los activos

- Cada activo tiene sus características, que difieren en el estado, en materia de seguridad, en los niveles de los subestados, confidencialidad, integridad y disponibilidad:
  - Subestado A (Autenticación)
  - Subestado C (Confidencialidad)
  - Subestado I (Integridad)
  - Subestado D (Disponibilidad)

ISO 27001: tipos de activo

- Se identifican 5 grandes tipos de activos de información:
  - El entorno del Sistema de Seguridad de la Información basado en ISO 27001.
  - El sistema de información en sí.
  - La información generada por la aplicación del Sistema de Seguridad de la Información.
  - Las funcionalidades de la organización, en las que se justifican las exigencias de los Sistemas de Información anteriores.
  - Otros activos, ya que el tratamiento realizado a los activos es un método de evaluación de riesgos que tienen que permitir la inclusión de cualquier otro activo.

ISO 27001: atributos de los activos

- Cada activo o grupo de activos desarrolla diferentes tipos de indicadores de valoración que ofrecen una orientación con lo que poder estimar el impacto que materializa la amenaza que puede provocar:
  - Un atributo cuantitativo, es decir, el valor del cambio que se puede emplear en ciertos tipos de activos y su utilidad.
  - Un atributo cualitativo, es decir, soporta la clasificación de los tipos de activos por su naturaleza.

ISO 27001: métrica de los activos

- Las personas responsables de proteger los activos tienen que identificar, definir y valorar todos sus activos. Las métricas de valoración se apoyan:
  - Los activos que se encuentran inventariados tienen una parte en activos relacionados con el entorno y otra parte con los sistemas de información.
  - Otros activos que pueden estar o no inventariados, suelen estarlo con las aplicaciones existentes que cubren la obtención de información.
  - Muchos otros activos no pueden ser inventariados en el sentido contable del término.

ISO 27001: métrica de los activos

- Subestado A (autentificación):
  - Baja: no se requiere conocer los activos de información.
  - Normal: es necesario conocer al emisor del activo.
  - Alta: es necesario evitar el repudio en destino.
  - Crítica: se requiere determinar la autoría y no-modificación de contenido.

ISO 27001: métrica de los activos

- Subestado C (Confidencialidad):
  - Libre: No tiene restricciones la hora de darle difusión.
  - Restrigida: presenta restricciones normales.
  - Protegida: tiene restricciones altas.
  - Confidencial: no se pude difundir bajo ningún concepto.

ISO 27001: métrica de los activos

- Subestado I (integridad):
  - Bajo: se puede reemplazar de una forma bastante fácil.
  - Normal: se puede reemplazar con un activo de calidad semejante con una molestia razonable.
  - Alto: la calidad necesaria del activo es reconstruible de forma fácil.
  - Crítico: no se puede volver a obtener una calidad semejante.

ISO 27001: métrica de los activos

- Subestado D (disponibilidad):
  - Menos de una hora.
  - Hasta un día laborable.
  - Hasta una semana.
  - Más de una semana.

ISO 27001: software de apoyo

ESCUELA DE COMERCIO
PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO

MÓDULO 4

PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

Prof. Mg. Rafael Mellado S.
rafael.mellado@pucv.cl
COM5163 – Sistemas de Información 3
Escuela de Comercio