BUSINESS ALLIANCE FOR SECURE COMMERCE

Cartilla
No. 6

En BASC estamos para ayudarle

Metodologías de Seguridad Informática

Consideraciones generales

Las empresas en el contexto de la cadena de suministro internacional y en general todas las organizaciones en los ambientes globalizados experimentan riesgos. Comprendemos desde BASC el riesgo como resultado de las incertidumbres a las que está expuesta una organización que experimenta amenazas a su capacidad estratégica para lograr sus objetivos y metas comerciales. Las actuales condiciones económicas derivadas de la crisis mundial por la emergencia sanitaria, han acentuado significativamente la materialización de ciberdelitos y riesgos a la estructura de Tecnología de la Información (TI), estos riesgos, son los desafíos que abordaremos en este documento desde el control operacional para la seguridad en TI.

La seguridad informática en el marco internacional para BASC se basa en los siguientes principios: identificar, proteger, detectar, responder y recuperar. Estos principios son la base para el actuar y evidenciar la gestión.

Conviene saber que actividades asociadas a las áreas de la empresa que se encuentren en red son más vulnerables a los intrusos y quienes son los atacantes más habituales. La tendencia consiste en confiar en los usuarios internos de la red de área local (LAN) y desconfiar de las conexiones que se originan en Internet o a través de módems de acceso telefónico y líneas dedicadas. Resulta importante confiar en los usuarios de la red y en el personal autorizado que utiliza los recursos internos de la red. La confianza también debe ser sopesada con la realidad. Es necesario restringir el uso de los equipos de la infraestructura de la red y los recursos vitales.

Cabe anotar que no todas las amenazas son maliciosas, pero pueden mostrar el mismo comportamiento y causar el mismo daño, independientemente de donde procedan. Es importante entender qué tipos de ataques y puntos débiles son los más comunes y qué hay que hacer a nivel normativo para garantizar un cierto grado de networking seguro.

Contenido

1. Metodología de Análisis de Riesgo

Según ISO 27005:2018 e ISO 31000:2018

Para abordar un procedimiento documentado con base en la gestión del riesgo y su rol en la cadena de suministro, cada líder de proceso asignado en la empresa BASC a liderar las unidades estratégicas de TI deben de definir la gestión de riesgos que puedan afectar la Seguridad de la información, en esta parte de este documento abordaremos lo que establece la ISO 27005 y la ISO 31000, normas de referencia para cumplir con este requerimiento de la norma BASC.

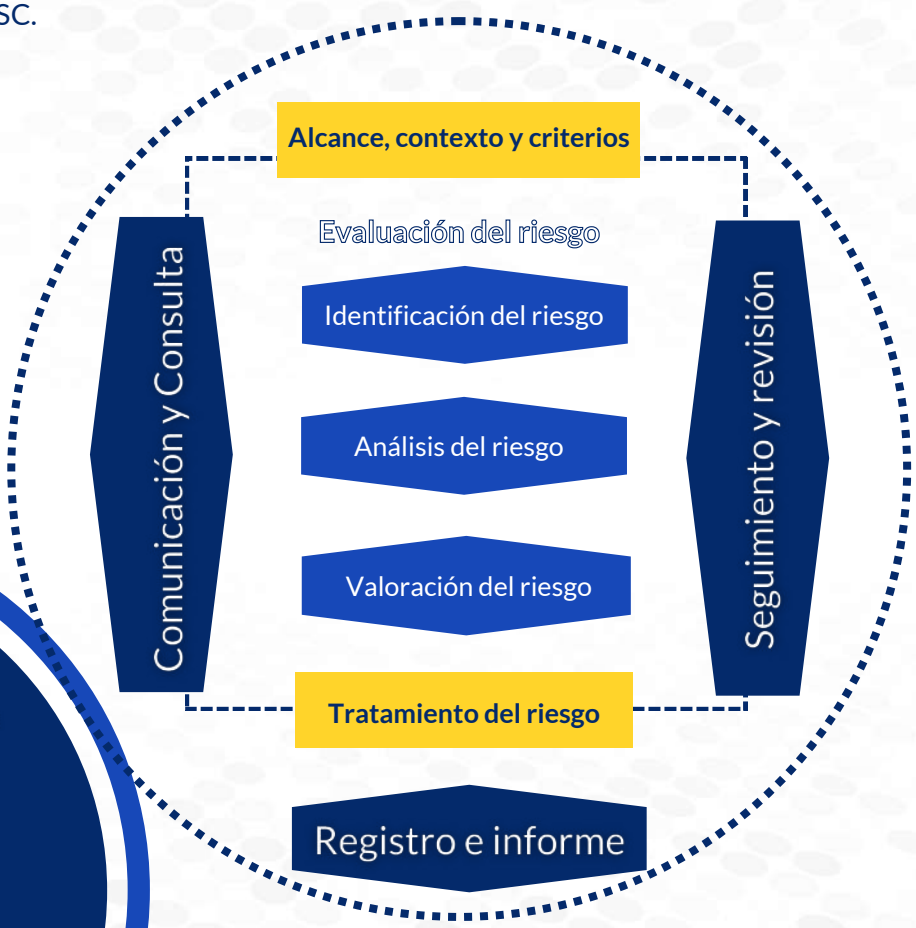


Figura N° 1. Proceso Gestión de Riesgo ISO 31000:2018

Nota: *El proceso de la gestión del riesgo debería ser una parte integral de la gestión, de la toma de decisiones y se debería integrar en la estructura, las operaciones y los procesos de la organización. Puede aplicarse a nivel estratégico, operacional, de programa. Para la Seguridad de la Información será un recurso para dar cumplimiento al requisito del estándar de la norma BASC.*

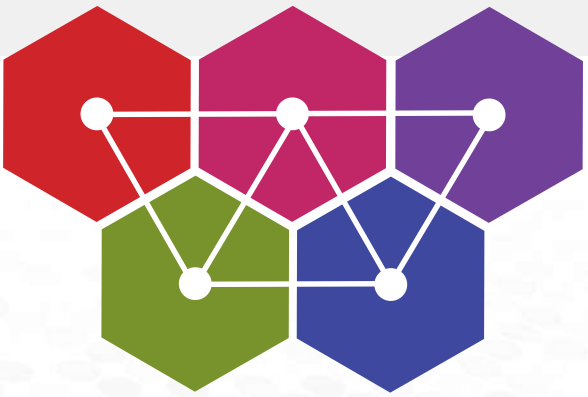
Te recomendamos la siguiente herramienta para que puedas empezar a desarrollar la gestión de riesgos:

Alcance, contexto y criterios	Identificación del riesgo	Análisis del riesgo	Valoración del riesgo
Identificar activos, a través de inventarios.	Identificar amenazas	Estimar probabilidad de ocurrencia, ver sector económico.	Estimar la priorización del riesgo
Valorar activos	Identificar vulnerabilidades	Identificar controles existentes documentados y no documentados.	Estimar estado del riesgo
Identificar la capacidad de **TI** implementadas en la empresa.	Identificar agentes generadores	Estimar impacto por materialización de amenazas.	
		Evaluar controles existentes.	

Tabla N° 1 Actividades a desarrollar de Gestión de Riesgos

Alcance, contexto y criterios

El fin de comprender el alcance, contexto y criterios para gestionar los riesgos de seguridad de la información tiene como propósito en el alcance comprender el límite que determina la alta dirección para aplicar esta estrategia de prevención a los recursos TI que posee la empresa para cumplir su misión. Los criterios definen los diversos recursos existentes dependiendo del tamaño de la organización y de lo robusto que sean sus recursos para cumplir de forma segura el propósito de la empresa y el contexto es la comprensión de los factores externos e internos que asociados a la estrategia de la organización se identifican que políticas, escenarios y amenazas, estos pueden afectar la continuidad de la operación de la empresa en cuanto se materialice o no un riesgo.



Actividades por realizar

- Definir Alcance, el contexto y Criterios de valoración de riesgos.
- Determinar criterios para valorar los riesgos y evaluar el riesgo de seguridad de la información de la empresa. para ello se puede considerar:

a. Qué valor tiene el proceso de información en la empresa desde la estrategia del negocio.
b. La criticidad de los activos de la información involucrados en las actividades de la organización.
c. En su empresa que tan importante es, operacionalmente para su negocio, la disponibilidad de la confidencialidad y la integralidad.
d. Las expectativas de sus partes interesadas frente a las consecuencias negativas al ser afectados por ciberdelito o por una pérdida de información.

Identificar activos de información

La identificación de los activos de la información es importante porque este es un factor para determinar los criterios de impacto, que se comprenden como los criterios de consecuencia que pueden afectar su negocio.

Un activo es de acuerdo con las Normas Internacionales de Información Financiera (NIIF) para PYMES, es considerado como un recurso controlado por la entidad como resultado de sucesos pasados y del cual espera obtener en el futuro beneficios económicos. También podemos precisar que un activo es: "cualquier elemento al cual se le asigna un valor y por tanto debe protegerse", lo cual puede entenderse igualmente como aquello que requiere la organización para el cumplimiento de sus objetivos.

- Tipos de activos
- Clases de activos

Activos de información y físicos		
Activos físicos	Infraestructura física	Oficinas
	Hardware	Servidores, dispositivos de comunicaciones, computadoras de escritorio.
	Tecnología Software	Aplicaciones
Activos de información	Electrónica	Información importante para el negocio
	Documentos	Información importante para el negocio.
Personal	Dueños o líderes de administrar información	Nivel directivo dueño de la información que asigna permisos para leer utilizar y modificar la información.
		Personal que utiliza la información para su trabajo.
Servicios		Correo electrónico

Tabla N°2 Activos de Información

Con base en la tabla anterior se empiezan a identificar el estado de los activos y hacernos las siguientes preguntas para identificar amenazas, las cuales tienen sus orígenes en el contexto definido en la organización:

¿Qué puede suceder?, ¿Por qué puede suceder? = agente generador y/o causas

¿Qué eventos evitan, dificultan o retrasan el logro de nuestros Objetivos?

¿Cuáles serían las consecuencias? = efectos

Como los activos de información los comprendimos como un criterio de impacto, deberían de definirse criterios en función del grado del daño o los costos para la organización generados por un evento de seguridad de la información considerando:

a. Nivel de identificación del activo de información impactada, ejemplo: se impacta el PC de un auxiliar de bodega o de un almacén por descargar un software para redes sociales u otros.
b. Incidencias de la seguridad de la información, ejemplo: pérdida de confidencialidad integridad y disponibilidad.
c. Operaciones deterioradas (internas y externas).

Valoración de los activos de información

Para Valorar los activos debemos de tener en cuenta tres elementos en nuestra metodología de gestión de riesgos en Seguridad Informática son: Confidencialidad, Integridad y Disponibilidad.

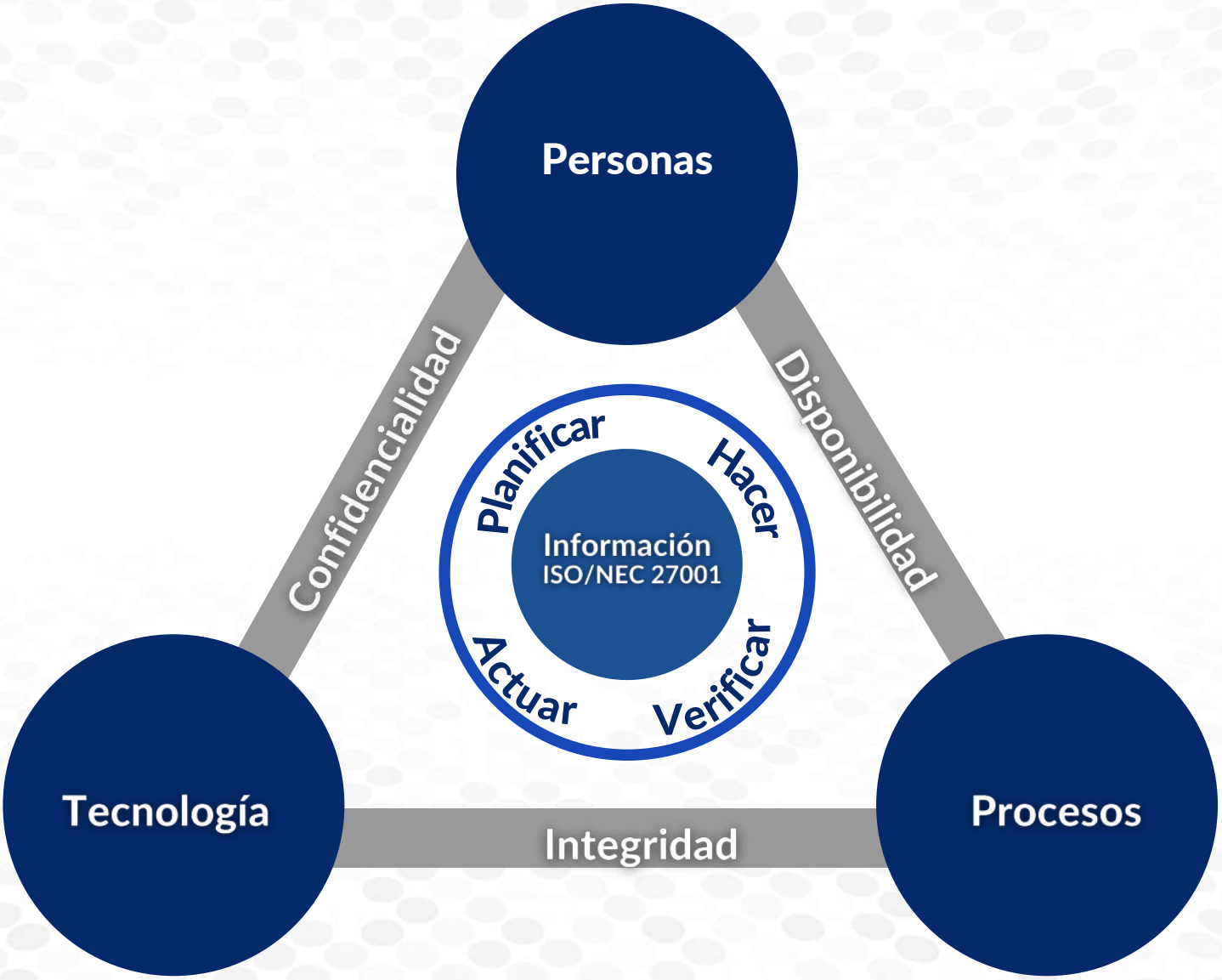


Figura N° 1. Pilares de la seguridad de la información ISO 27001:2013.
Fuente: LinkedIn Carlos A. Martínez Ramírez - Technical Leader en Olimpia IT

a. Confidencialidad:

Los activos de información reciben una valoración alta cuando su nivel de confidencialidad es mayor, teniendo en cuenta que la divulgación no autorizada de la misma puede afectar en alguna medida los intereses, imagen y operación de la compañía.

Para realizar la valoración de los activos en la dimensión de confidencialidad tendremos en cuenta los resultados obtenidos en la herramienta para clasificación de información, (con base en la clasificación obtenida para cada activo asignaremos un valor).

Clasificación	Valor
Pública	5
Uso interno	10
Confidencial	15
Reservada	20

Tabla N° 3. Valoración de la confidencialidad

b. Integridad:

Los activos son valorados con mayor valor cuando su alteración puede generar daños graves a la organización.
La valoración en la dimensión integridad se realizará utilizando los siguientes criterios, como se muestra en la tabla N° 4.

Para calcular el valor del activo se realiza la sumatoria de todos los factores evaluados y se establecerá el valor de activo como se relaciona en la tabla N°5.

Clasificación	Valor
Información que afecta mucho la operación.	20
Información que afecta moderadamente el negocio.	15
Información que puede tener algunos errores o cambios sin afectar su sentido principal.	10
Información o activos que pueden tener errores sin tener impactos al negocio.	5

Tabla N°4. Criterios para la valoración de la integridad

c. Disponibilidad:

Los activos de una determinada organización tendrán mayor valor en la medida que si no están disponibles se impactará gravemente el negocio. Igualmente, un activo que al no estar disponible no afecte de ningún modo el negocio, tendrá un menor valor.
Para determinar el impacto que sobre el negocio genera la indisponibilidad del activo se utilizarán los criterios relacionados en la siguiente tabla:

Valoración de activo	Sumatorio de los valores considerados
MB: muy bajo	De 14 a 24
B: bajo	De 25 a 35
M: medio	De 36 a 46
A: alto	De 47 a 57
MA: muy alto	De 58 a 68

Tabla N° 5. Valoración de la confidencialidad del activo.

Valoración de los activos	Mínimo 1	Medio 3	Grave 5	Catastrófico 7
Las pérdidas económicas por indisponibilidad del activo son: Los servicios prestados se ven afectados por la indisponibilidad del activo de la siguiente forma:	Interrupción leve o nula en suministro de servicios.	Obliga al cliente a cambiar de proveedor de forma transitoria.	Pérdida de algunos clientes de forma definitiva.	Pérdida de clientes claves
La indisponibilidad del activo afecta la operación así:	Retrasos en funciones no vitales	Retrasos leves en funciones vitales	Retrasos graves en funciones vitales	Interrupción inmediata de funciones vitales
La indisponibilidad del activo afecta la imagen en el sentido que:	No afectar la confianza en los productos o servicios.	Pérdida de confianza en un servicio específico o en una parte de la organización.	Pérdida de confianza de parte de los clientes.	Pérdida de confianza del mercado y daños a la imagen de marca.
La indisponibilidad activo afecta cumplimiento obligaciones sentido que:	Produce una falta leve en el cumplimiento de algún contrato.	Produce una falta en el cumplimiento de algún contrato que obliga a renegociar.	Produce una falta grave en el cumplimiento de algún contrato.	Deja a la organización al margen de la ley

Tabla N° 6. Criterios para valoración de disponibilidad

Se asigna un valor utilizando la siguiente escala:

Tabla N° 7. Valoración de la disponibilidad.

Valoración	Valor
Mínimo	1
Medio	3
Grave	5
Catastrófico	7

Identificación de amenazas posibles:

Las amenazas son resultados de actos deliberados que pueden afectar nuestros activos o los activos de información, sin embargo, existen eventos naturales o accidentales que deben ser considerados por su capacidad de generar incidentes de seguridad.

Causa	Evento o amenaza
Eventos naturales	Terremotos, huracanes, desbordamientos de ríos que afecten la infraestructura física
Eventos externos	Pérdida de proveedores, problemas de transporte, sobrecargas
Condiciones Internas	Problemas de transporte
Actos deliberados	Fallas de hardware, fallas de software, fallas en la red
Actos accidentales	Destrucción de información, incendios
Humano	Epidemias, indisponibilidad de personal

Tabla N° 8. Listado de amenazas

Identificación de vulnerabilidades de los activos:

Debe identificarse la forma como cada una de las amenazas podría materializarse, es decir, que vulnerabilidades permiten que las amenazas se conviertan en situaciones de riesgo reales.

Algunos tipos de vulnerabilidades

·Ausencia de políticas de Seguridad de la Información.
·Configuraciones no seguras.
·Empleado descontento (Salario emocional, monetario).
·Empleado deshonesto (fraude, corrupción, sobornado o víctima de chantaje).
·Errores de configuración.
·Falta de actualizaciones.
·Uso de servicios inseguros.
·Uso de protocolos inseguros.
·Cultura de inseguridad procesos.

Analizar los Riesgos sobre los Activos:

Establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos, a fin de determinar la capacidad de la organización para su aceptación o manejo.

Estimar el Impacto sobre los Activos:

El impacto es la medida de daño causado por un incidente en el supuesto de que ocurra, afectando así, el valor de los activos esta pérdida de valor la denominamos degradación del activo.

La medición del impacto la realizaremos utilizando la siguiente matriz:

Valoración del activo	Afectación del activo				
	5%	25%	50%	75%	100%
MA: Muy alto	A	A	A	A	MA
A: Alto	M	M	A	A	A
MA: Muy alto	B	M	M	A	A
M: Medio	MB	MB	M	M	M
MB: Muy bajo	MB	MB	MB	B	M

Tabla N°9. Matriz de estimación del impacto sobre activos.

La estimación del impacto puede ser entonces:

1. **MA: Muy alto**
2. **A: Alto**
3. **M: Medio**
4. **B: Bajo**
5. **MB: Muy bajo**

Estimar probabilidad de ocurrencia

La probabilidad de ocurrencia se calcula con base en la siguiente tabla:

Valor	Ocurrencia	Frecuencia
Es probable que se materialice la amenaza a diario	100	Muy frecuente
Es probable que se materialice la amenaza semanalmente	10	Frecuente
Es probable que se materialice la amenaza anualmente	1	Normal
Es probable que se materialice la amenaza cada varios años	1/10	Poco frecuente

Tabla N°10. Valoración cuantitativa de la frecuencia

a. Cuantitativo: a partir de los datos históricos que la organización haya acumulado en el tiempo. La frecuencia se considera como número de ocurrencias de la amenaza en un año.

Frecuencia	Probabilidad
Más de 100 al año	Muy frecuente
Entre 10 y 20 al año	Frecuente
Entre 1 y 5 al año	Normal
Menos de 1/10 al año	Poco frecuente

TABLA N°11. Valoración de la frecuencia

Estimar riesgos

Conociendo el impacto de las amenazas sobre los activos es posible determinar el nivel de riesgo, teniendo en cuenta la frecuencia de ocurrencia de los incidentes.

IMPACTO					
	MA: muy alto	**Zona de riesgo importante**	**Zona de riesgo importante**	**Zona de riesgo importante**	**Zona de riesgo inaceptable**
	A: alto	Zona de riesgo moderado	Zona de riesgo moderado	**Zona de riesgo importante**	**Zona de riesgo importante**
	M: medio	Zona tolerable del riesgo	Zona de riesgo moderado	**Zona de riesgo importante**	**Zona de riesgo importante**
	B: bajo	Zona aceptable del riesgo	Zona tolerable del riesgo	Zona de riesgo moderado	Zona de riesgo moderado
	MB: muy bajo	Zona aceptable del riesgo	Zona aceptable del riesgo	Zona tolerable del riesgo	Zona tolerable del riesgo
		Poco frecuente	Normal	Frecuente	Muy frecuente

FRECUENCIA

Tabla N° 12. Matriz para determinación de riesgos – mapa de calor.

Identificar controles existentes

Los controles existentes son las medidas implementadas con las que la empresa implemento los recursos en TI, con el fin de mitigar la exposición a los riesgos, estos son implementados con o sin una metodología. Los controles se manifiestan en procedimientos, instructivos, consignas, políticas, directrices o mecanismos tecnológicos entre otros.

Para realizar una evaluación de los controles existentes puede utilizarse como referencia el anexo A del estándar ISO/IEC 27001/2013. El cual referencia un número considerable de controles en cada una de las áreas de la Seguridad de la Información.

Evaluar los controles existentes

Una vez identificados los controles existentes es necesario evaluar su efectividad frente a los riesgos que se pretenden mitigar. Para medir la efectividad de los controles utilizaremos los siguientes criterios:

Evaluación de control	Valores				
El control está formalmente establecido.	Nulo	Deficiente	Regular	Bueno	Excelente
El control está perfectamente desplegado, configurado y mantenido.	0%	25%	50%	75%	100%
Existen procedimientos claros de uso del control y en caso de incidencias.	0%	25%	50%	75%	100%
Los usuarios están formados y concienciados sobre la aplicación del control.	0%	25%	50%	75%	100%
El control es funcional desde el punto de vista teórico y operacional.	0%	25%	50%	75%	100%

Tabla N°13. Criterios para valoración de controles existentes.

La eficiencia del control se estima con base en la siguiente tabla:

Efectividad = Promedio de las valoraciones realizadas

Suma	Efectividad del control
Mayor de 89%	Excelente
De 65% y 89%	Bueno
De 40% y 64%	Regular
De 15% y 39%	Deficiente
Menor de 15%	Nula

Tabla N° 14. Valoración de controles.

Valoración de Riesgos

Objetivo
Determinar el nivel o grado de exposición de la organización a los impactos del riesgo, estimando las prioridades para su tratamiento.

Estimar riesgo
El riesgo se establece considerando los controles existentes, orientados a prevenir que el incidente se presente.

Controles orientados a prevenir el incidente:

En la Figura N° 2 se aprecia como a medida que la efectividad del control aumenta, la frecuencia de ocurrencia de incidentes disminuye.

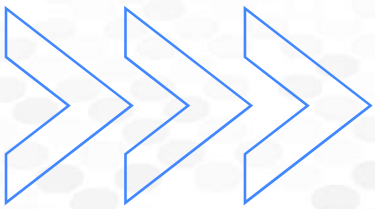


Figura N°2. Efectividad de control y frecuencia.

Controles que limitan la degradación de activos:

EFECTIVIDAD DEL CONTROL

Nada *Deficiente* *Regular* *Buena* *Excelente*

Figura N°3. Efectividad de control y degradación.

A: alto *M: medio* *B: bajo* *MB: muy bajo*

DEGRADACIÓN DE ACTIVOS

En la figura No 3, se aprecia que la efectividad del control aumenta, la degradación del activo es menor.
Si los controles tienen niveles adecuados de efectividad la degradación de los activos o la frecuencia de los incidentes debe ser menor a los valores hallados inicialmente.

Priorizar los riesgos sobre los activos

El riesgo nos muestra el grado de exposición frente a las amenazas evaluadas, es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables, y establecer la prioridad de las acciones requeridas para su tratamiento. Las acciones que se deben ejecutar se harán con base en la siguiente tabla:

Riesgo	Prioridad	Tiempo de ejecución de acciones
Inaceptable	Muy alta	Inmediata
Importante	Alta	De 0 a 4 meses
Moderado	Media	De 4 a 7 meses
Tolerable	Baja	De 7 a 12 meses
Aceptable	Muy baja	De 12 a 16 meses

Tabla N° 15. Priorización de riesgos.

Gestión de riesgos en los activos

Objetivo

Estructurar los criterios para la toma de decisiones respecto al tratamiento de los riesgos, en esta etapa se establece las guías de acción necesarias para coordinar y administrar los eventos que pueden comprometer la confidencialidad, integridad y disponibilidad de los activos.

Desarrollo de actividades:

Toma de decisiones

Si el riesgo se ubica en la Zona de Riesgo Aceptable, permite a la organización aceptarlo, es decir, el riesgo se encuentra en un nivel que puede asumirse sin necesidad de tomar otras medidas de control.

Si el riesgo se ubica en la Zona de Riesgo Inaceptable, es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible.

Si el riesgo se sitúa en cualquiera de las otras zonas (riesgo tolerable, moderado o importante) se deben tomar medidas para llevar los Riesgos a la Zona Aceptable, con la implementación de los respectivos controles.

Las medidas dependen del punto en la cual se ubica el riesgo:

Zona	Impacto	Frecuencia	Medida
Zona de riesgo importante	MA: muy alto	*Poco frecuente*	Prevenir riesgo: Implementar controles frente a impacto.
	MA: muy alto	*Normal*	
	A: alto	*Frecuente*	Prevenir riesgo: Implementar o mejorar controles frente a impacto y frecuencia.
	M: medio	*Frecuente*	
	M: medio	*Muy frecuente*	
Zona de riesgo moderado	A: alto	*Poco frecuente*	Compartir riesgos. Prevenir riesgo: Implementar o mejorar controles frente a impacto.
	A: alto	*Normal*	Prevenir riesgo: Implementar o mejorar controles frente a impacto y frecuencia.
	M: medio	*Normal*	
	B: bajo	*Frecuente*	**Realizar análisis costo- beneficio para decidir si el riesgo se asume, se previene o se comparte.**
	B: bajo	*Muy frecuente*	
Zona tolerable del riesgo	M: medio	*Poco frecuente*	Prevenir riesgo: Implementar ó mejorar controles frente a impacto.
	B: bajo	*Normal*	**Realizar análisis costo- beneficio para decidir si el riesgo se asume, se previene o se comparte.**
	MB: muy bajo	*Frecuente*	
	MB: muy bajo	*Muy frecuente*	

Tabla N° 16. Estimación de los riesgos sobre los activos.

La selección de controles se realizará tomando como referencia el Anexo A del estándar ISO/IEC 27001:2013.

Para seleccionar los controles frente a los riesgos establecidos, deberá realizarse un análisis costo-beneficio para evitar implementación de controles con costos superiores al costo de los riesgos reales.

Plan de tratamiento de riesgos

Una vez seleccionados los controles que serán implementados para la mitigación de riesgos es necesario elaborar un plan de acción que garantice un efectivo despliegue de los mismos.
La elaboración del plan de tratamiento de riesgos será responsabilidad del Oficial de Seguridad Informática y la respectiva aprobación de los mismos del Comité de Seguridad.

Tratar el riesgo implica identificar opciones como:

a. Evitar el riesgo.
b. Reducir probabilidad.
c. Reducir las consecuencias o impactos.
d. Transferir el riesgo.

Para ello hay que evaluar opciones de tratamiento como lo indicamos anteriormente frente al costo-beneficio.

Preparar planes de tratamiento pueden considerar planes de contingencia y emergencia en SI aplicados a TI.

Es importante señalar que si los riesgos no se ubican en el mapa de valor en las categorías de riesgos bajos o aceptables, se tratan utilizando las opciones consideradas ya sea en los controles o documentar las existentes si no se encuentran descritas.

Esto implica que los riesgos en la posición descrita en este párrafo requieren monitorear permanentemente cuando son de baja prioridad.

Como se documenta un Tratamiento:

Tratamiento es = Acciones + Responsables + Cronogramas + Monitoreo.

Tratamiento del riesgo	
Opción	**Descripción**
Prevenir	a. No hacer nada. b. Eliminar la actividad que genera el riesgo. c. Sustituir por otra menor peligrosidad.
Evitar	a. Anticiparse. b. Procedimientos. c. Políticas de SI en TI. d. Capacitación y entrenamiento. e. Auditoria de control.
Proteger	a. Medidas sobre los recursos amenazados. b. Planes de manejo de crisis. c. Continuidad de negocio.
Transferir	a. Trasladar las pérdidas a otra empresa. b. Contratos: Servicios de transporte, vigilancia, alojamiento en iCloud, NAS.
Aceptar	a. Asumir consecuencias. Impacto Leve Frecuencia baja. b. No hay medidas disponibles.
Retener	a. Cautivas. b. Destinación de fondos para cubrir consecuencias. c. Líneas de financiación o de crédito Provisiones contables.

Tabla N°17 aparecen las opciones de tratamiento con la descripción de estos.

Para definir la mejor alternativa para administrar y mitigar los riesgos, la compañía debe tomar en cuenta los siguientes aspectos y posteriormente establecer la estrategia:

a. **Beneficios:** al implementar el tratamiento de riesgo.
b. **Costo:** de la implementación del tratamiento de riesgo seleccionado.
c. **Esfuerzo:** requerido para la implementación del tratamiento del riesgo, tiempo para impactar la gestión del proceso a través de la implementación del tratamiento del riesgo.

Implementación del tratamiento

a. Concretar y evidenciar las acciones.
b. Es un instrumento de planeación estratégica y facilita el direccionamiento.
c. Es útil para la ejecución de acciones preventivas, correctivas y de mejoramiento.
d. Facilita el seguimiento y el control a la gestión de los riesgos.
e. Facilita la formulación de las políticas de tratamiento de riesgos.

Monitorear los riesgos

- La efectividad del plan de tratamiento de los riesgos, las estrategias y el sistema de administración que se establezca para controlar la implementación es un factor determinante para medir si lo documentado en el tratamiento contribuye para mejorar la gestión del riesgo.
- Revisar sobre la marcha para asegurar que el plan del tratamiento se mantiene relevante y es pertinente.
- Monitorear y revisar el desempeño del sistema de administración de riesgos y los cambios que podrían afectarlo.
- Repetir y revisar regularmente el ciclo de administración de riesgos.

Monitoreo, revisión y seguimiento

- Establecer periodicidad para la revisión de los riesgos.
- Verificar el cumplimiento y efectividad de las acciones establecidas en el plan de tratamiento.
- Identificar nuevos riesgos.
- Dar cumplimiento a los cronogramas de seguimiento.

Comunicación

- Uno de los recursos relevantes en la gestión de riesgos es la participación, ello se logra con la comunicación asertiva y directiva.
- Proceso de construcción y tratamiento participativo y colectivo.
- Plan de comunicación de los Riesgos.
- Establecer Mecanismos para la percepción de los riesgos a nivel interno y externo

2. Manejo de la información y uso de recursos informáticos

Para establecer el manejo de la información y uso de los recursos informáticos con el fin de minimizar los riesgos que vimos antes que pueden afectar la pérdida de información, aumentar los niveles de eficiencia y productividad de los funcionarios de su organización se busca prolongar la vida útil de los equipos de cómputo y aprovechar al máximo las herramientas TI y los Sistemas de información. Los recursos para cumplir este objetivo son, la documentación, divulgación y medición de políticas en SI.

Políticas Seguridad Informática requeridas por BASC

Para abordar el primer elemento que trae el estándar, referenciamos a la norma internacional ISO 27002: 2017 que junto a las políticas son comprendidas como la declaración de compromiso que hace la alta dirección para desarrollar los procedimientos, identificar roles, responsabilidades y desarrollar una cultura corporativa basada en el control.

La empresa debe establecer e implementar:

a. Una política para impedir que se revele información confidencial.
b. Una política de uso de los recursos informáticos.

Guía de implementación:

La empresa debería definir una política de seguridad de la información al nivel de la alta dirección que establezca un enfoque alineado a la estrategia de la organización y que contenga la forma de gestionar los objetivos estratégicos en seguridad de la información.

La política de seguridad de la información debería considerar declaraciones pertinentes relativas a:

a. La definición de la seguridad de la información, de forma que determine la forma de prevenir la revelación de la información confidencial.

b. Principios para orientar las actividades determinadas a revelar información, al uso de los recursos informáticos.

c. Asignar responsabilidades generales y particulares en materia de gestión de la seguridad de la información.

d. Los procesos para señalar las actividades para gestionar las no conformidades, correcciones y exclusiones que apliquen a esta política.

Ejemplos de estas políticas deben considerar en su contenido los controles:

1. Control de acceso a los recursos TI de la organización.
2. Seguridad física de lugares de alojamiento de la información, (controles a oficinas, despachos, lugar de almacenamiento de servidores, protección contra amenazas externas de CCTV).
3. Áreas de acceso a equipos que salen de la compañía, equipo informático de usuario desatendido.
4. Reutilización o retirada de dispositivos de almacenamientos.
5. Uso de memorias USB, pen drive.
6. Seguridad del cableado.
7. Temas relacionados a los usuarios finales como pueden considerarse:

- La forma en que van hacer uso de los activos TI.
- La forma en como transfieren información asociada a su actividad y gestión dentro de la organización.
- Restricción de aplicaciones y software no licenciado.
- Uso de dispositivos móviles.
- El teletrabajo y uso de dispositivos en casa u otro lugar fuera de la empresa.

Las políticas son muy importantes para que los funcionarios de la empresa, comprendan la forma en que se establecen los controles, las funciones y responsabilidades.

Organización de la Seguridad de la Información SI

Las políticas como lo hemos visto es un recurso para establecer un marco de gestión para controlar la implementación y operación de la seguridad de la información que requiere una empresa, para ello se deben definir roles y responsabilidades relacionadas con la seguridad de la información y estas se hacen de acuerdo con las políticas definidas.

Ejemplo:
Responsabilidades para:

1.Protección de los activos en TI entregados a cada usuario.

2.Actividades de gestión en materia de identificación de riesgos de SI que identifiquen los usuarios al interactuar con los recursos TI como son virus, accesos no autorizados, copias de archivos entre otros.

3.Uso adecuado del hardware y software implementado en los procesos de la organización.

4. Propiedad intelectual del software y demás recursos que requieran cumplimiento de este aspecto legal.

5. Si los sujetos de la organización deciden delegar claves en otros. ellos deben comprender que esta práctica no los exime de su responsabilidad deberían validar que todas las tareas delegadas a sus colaboradores deben ser correctamente ejecutadas.

6. Mantener la competencia en el uso de los aspectos de seguridad de la información implementados en la empresa; si los trabajadores requieren de conocimiento para ejecutar un procedimiento relacionado en los ambientes de SI, los trabajadores deben de actualizar sus competencias en relación con estos procesos y evaluar continuamente la aplicación correcta de las actividades asignadas en SI.

7. Designar los aspectos relativos en la supervisión de proveedores y personal externo que suministre recursos relacionados a la seguridad de la información de la empresa. Si un funcionario tiene la labor de negociar con proveedores, este debe documentar los controles en esta actividad de coordinación.

Gestión de activos TI

La organización debería de garantizar la SI en el teletrabajo, para ello podría considerar adoptar políticas y medidas de control para proteger los recursos TI contra los probables riesgos en la utilización de estos dispositivos fuera de las instalaciones.

Para implementar este aspecto se recomienda:

1. Control de los dispositivos móviles asociados al teletrabajo, donde se registre un estado de este recurso.

2. Requisitos para la protección física, considerar pólizas contra hurto o daño de componentes técnicos como software.

3. Las restricciones de instalación de software.

4. Los requisitos para la actualización de los cookies, parches o actualizaciones de software.

5. La restricción a servidores externos, junto a la de conexiones a otros dispositivos diferentes a los establecidos en la empresa.

6. Los controles de acceso.

7. La protección contra malware o software malicioso.

8. La inhabilitación, el eliminado o borrado de archivos de la organización.

9. El proceso de copia de respaldo .

10. La utilización de servicios y aplicaciones web que expongan la seguridad del equipo.

En el teletrabajo es recomendable implementar una medida de seguridad adecuada para preservar la información a la que se accede, la información que se almacena en dispositivos externos

Se recomienda adicionalmente:

a. Manejar en el teletrabajo un entorno físico adecuado, libre de riesgos o exposición a vulnerar la seguridad del equipo o dispositivo móvil.

b. Al facilitar un acceso al escritorio virtual a través de una VPN a cualquiera de los recursos TI de la empresa de forma remota, considerar las condiciones seguras mínimas autorizadas por el área de TI.

c. La amenaza de un intento de acceso sin autorización a la información de los recursos Ti de la empresa por parte de personas del mismo lugar de teletrabajo, ejemplo familia y amigos.

d. Las reglas y directrices para el acceso de la familia y los accesos de los visitantes al equipo y a la información de la compañía.

e. La provisión de soporte y mantenimiento de hardware y software por parte de técnicos autorizados por la empresa.

f. Los procedimientos de las copias de seguridad que permitan una adecuada continuidad de negocio y los roles del usuario.

g. La forma de revocar la autorización y acceso del equipo en caso de pérdida o cuando se termine las actividades de teletrabajo.

Clasificación de los datos en la seguridad de la información

La información para la empresa constituye uno de los activos significativos, para ello es necesario asegurarse de definir un nivel adecuado de protección de acuerdo con sus atributos como pueden ser importancia para la empresa.

Para clasificar la información la empresa debe considerar:

a. Los requisitos legales asociadas a la información, ejemplo ley de habeas data 1266 de 2008.

b. La criticidad ante la revelación o modificación sin autorización, que exponga la continuidad de negocio, secretos comerciales, patentes entre otros.

c. La clasificación debe ser determinada desde el contexto de la empresa, las necesidades y expectativas de los asociados de negocio en cuanto a entregar y tratar la información en la que se vean inmersos estos.

d. LA clasificación debería definir a los responsables en los diferentes procesos de la empresa, estos son los adecuados para definir su clasificación.

e. Definir un esquema o método de clasificación donde se pueda considerar: criterios para clasificar la información, para revisarla, en el tiempo. Estos pueden ser: el nivel de confidencialidad, integridad y disponibilidad. Este debe estar alineado a la política de SI y los principios de TI.

f. Una buena práctica en clasificar la información es involucrar al ecosistema de SI y esto se hace involucrando transversalmente a todos los usuarios del recurso TI de manera que las personas que tienen contacto con la información y activos comprendan la importancia de proteger y aplicar la protección planteada en los controles de esta clasificación.

g. Los resultados de la clasificación finalmente deberán arrojar un recurso documentado que indica la aplicación transversal a todos los procesos, una evaluación en función de la sensibilidad, criticidad, confidencialidad, disponibilidad y integridad.

La manipulación de la información:

Este es un factor que se recomienda definir en compañía de la clasificación de la información, la empresa debería redactar información documentada para el manejo, tratamiento y comunicación de la información. De acuerdo con los expertos en la materia ISO 27001:2013; se recomienda contemplar:

a. Restricciones de acceso que dan apoyo a los requisitos de protección para cada nivel de clasificación.
b. Mantenimiento de un registro formal de receptores autorizados de los activos.
c. Protección de copias, sean temporales o permanentes, de información, a un nivel consistente con la protección de la información original.
d. Almacenamiento de activos de TI conforme a las especificaciones de sus fabricantes.
e. Marcado claro en todas las copias de soportes para la debida atención del receptor autorizado.

Activo	Descripción
Hardware	Estaciones de trabajo, computadores portátiles, impresoras, enrutadores, switches, módems, firewalls.
Software	Programas fuente, programas de objeto, utilidades, programas de diagnósticos, sistemas operativos, programas de aplicación y programas de comunicación.
Datos	Datos almacenados online y archivados offline, copias de seguridad, registros de auditorías, base de datos y datos en tránsito sobre los medios de comunicación.
Personas	Usuarios del sistema, administradores del sistema y mantenedores del hardware.
Documentación	Procedimientos, formularios, manuales e instructivos de procesos operativos y administrativos.

Tabla N° 18 Activo de red.

El inventario de los activos de la empresa debe ser dirigido conjuntamente con el fin de, garantizar el manejo y la evaluación coherentes de los activos corporativos.

Clasificación de los datos

La clasificación de los datos en función de los distintos niveles de importancia puede ser un paso preliminar a la hora de establecer su valor. Un sistema sencillo de alto, medio y bajo puede ser el punto de partida que sirva para evaluar la importancia relativa de los datos. Los datos pueden adoptar múltiples formas, entre las cuales se incluyen las siguientes:

·**Datos administrativos:** La correspondencia y otra información similar, como los registros y la información que esté a disposición del público.

·**Datos financieros:** Información del presupuesto, de la contabilidad y en general relativa a los ingresos y gastos de las operaciones corporativas.

·**Datos de cliente:** Información relacionada con el cliente que es de naturaleza persona lo información desarrollada fruto de encuestas, entrevistas, auditorías, observaciones o recomendaciones.

·**Datos de investigación:** Información de apoyo de la actividad de investigación de una empresa.

·**Datos exclusivos:** Información que no puede ser revelada al público sin el permiso del propietario.

La siguiente tabla muestra cómo se pueden clasificar los distintos tipos de datos y aplicar una clasificación en función de su importancia

Tipos de datos	Clasificación	Importancia
Resultados de auditorías	Investigación	Alta
Estadísticas de clientes	Investigación	Media
Memorandos corporativos	Administrativo	Baja
Datos de adquisición	Contabilidad	Alta
Secretos comerciales	Exclusivos	Alta
Salario de empleados	Contabilidad	Media

Tabla N° 19 clasificación de datos

3. Elementos de una arquitectura segura

El marco global debe incluir los siguientes elementos de una arquitectura de seguridad:

·Identidad:

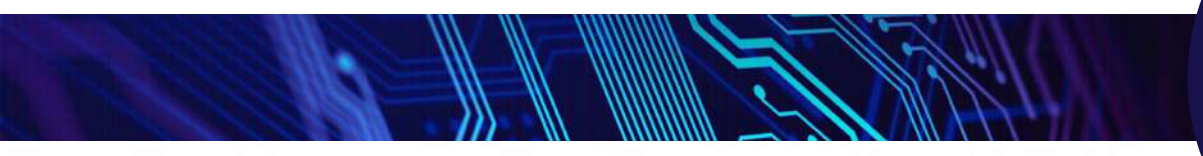
La identidad se define como el elemento de la arquitectura de seguridad que abarca la autenticación y la autorización. La autenticación responde a la pregunta ¿Quién es usted y dónde está? La autorización responde a la pregunta ¿A qué se le permite acceder? En necesario desplegar con precaución los mecanismos de identidad, ya que incluso las normas de seguridad más ciudades pueden ser omitidas si las implementaciones son difíciles de usar. Un ejemplo clásico es el de las contraseñas garabateadas en una nota y pegados en el monitor del computador o en el teléfono (una solución real para el usuario que tenga que recordar muchas contraseñas) Otro ejemplo de seguridad mal implementada se da cuando los usuarios de la red utilizan una contraseña de fácil adivinación para no tener que escribirla: el nombre de un hijo, el nombre del perro, el nombre del esposo, el nombre de la esposa, entre otros. Las empresas deben crear restricciones apropiadas dentro de sus sistemas, de forma que los intrusos que accedan a una parte del entorno corporativo no tengan acceso automático al resto del entorno.

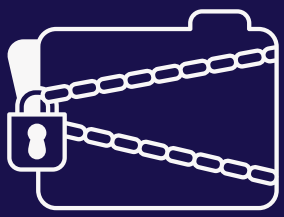
• Integridad:

La integridad es el elemento de la arquitectura de seguridad que abarca la seguridad de los dispositivos de la infraestructura de red (acceso físico y acceso lógico) y la seguridad del perímetro de red. El acceso físico a una computadora (o router, o switch o firewall) suele proporcionar a un usuario avezado un control total sobre este dispositivo. El acceso físico a una red suele permitir a una persona pulsar el enlace, bloquearlo o inyectar tráfico en él. Por lo tanto en la red LAN, la seguridad física deberá estar basada en control físico de acceso a personal no autorizado, circuitos cerrados de televisión y sistemas de acceso mediante claves encriptadas. Con estas medidas, las empresas pueden estar seguras de que en sus dependencias físicas, los activos están protegidos y que se mantiene una productividad de usuario alta. La seguridad del perímetro trata sobre la funcionalidad de tipo firewall, determinando que tráfico se permite o deniega en las distintas áreas de le red LAN. Los firewalls están colocados entre Internet y la red LAN, o entre la conexión de acceso telefónico y la red LAN.

·Confidencialidad:

La confidencialidad es el elemento de la arquitectura de seguridad que garantiza la privacidad de la comunicación de los datos entre el remitente y el destinatario de la información. Unas normas de seguridad estrictas deberán dictar a los usuarios que tipo de información sensible deberán ir cifrados. Independientemente del nivel en que se dicten las normas, la decisión de usar el cifrado deberá ser tomada por la autoridad de la empresa que sea la responsable de garantizar la protección de la información sensible.





·Disponibilidad:

La disponibilidad es el proceso de garantizar que todos los recursos vitales son accesibles. Mantener los datos disponibles significa que deberá haber una planificación de las actualizaciones del sistema y de los cambios en la configuración que estén probados para evitar sorpresas catastróficas causadas por errores o malas configuraciones del software.

·Auditoría:

El elemento de auditoría de la arquitectura de seguridad es necesario para verificar y controlar las normas de seguridad corporativas. Una correcta auditoría verifica la implementación completa de las normas de seguridad en la infraestructura de la red LAN.

El registro y el control subsiguientes de los eventos puede ayudar a detectar los comportamientos inusuales y las posibles intrusiones.

Para probar la eficacia de la infraestructura de seguridad, la auditoría de seguridad deberá tener lugar frecuentemente y a intervalos regulares. La auditoría deberá incluir nuevas comprobaciones de la instalación del sistema, métodos para descubrir posibles actividades maliciosas de intrusos, la posible presencia de un tipo de problemas específico (ataque DoS) y el cumplimiento general de las normas de seguridad del sitio.

Es posible usar un registro de auditoría, generado por todos los sistemas operativos que se ejecuten en la infraestructura para determinar el alcance del daño causado por un ataque.

Los rastros de auditoría suelen entrar en escena una vez que se sabe lo que ha ocurrido durante la evaluación del daño. El hecho a evitar es el de registrar todos y cada uno de los eventos, ya que esto se hace insostenible.

Si se registran demasiados datos y de produce una intrusión, esta intrusión quedará registrada (junto a los cientos de eventos no significados). Lo más probable es que la intrusión no se detecte por los responsables de detectar estas cosas, ya que estará oculta bajo una montaña de datos generados por el sistema.

Protección del entorno

Es preciso instalar e implementar protecciones del entorno apropiadas con el fin de proteger los recursos de red vitales. La importancia del sistema determina si la seguridad es o no adecuada. Cuanto más importante sea un sistema, más protecciones deberán implementarse para asegurar que el recurso está disponible a cualquier costo. Como mínimo, deberá garantizar las siguientes protecciones del entorno:

- *Prevención, detección, supresión y protección contra incendios.*
- *Prevención, detección y control de inundaciones.*
- *Protección del suministro eléctrico.*
- *Control de la temperatura.*
- *Control de la humedad.*
- *Protección frente a desastres naturales provocados por terremotos, rayos, tormentas, etc.*
- *Protección frente a campos magnéticos excesivos.*
- *Buenos procedimientos de limpieza para la protección contra la suciedad y el polvo.*

Protección de la autenticación

Es común encontrar en las empresas mecanismos de autenticación en contraseñas estándar y reutilizables. Cualquier contraseña reutilizable está expuesta a los ataques de escucha ilegal de programas sniffers (husmeadores). Conviene que en la medida de lo posible, estos entornos adopten un esquema de autenticación más sólido con respecto al manejo de las contraseñas. A continuación se enumeran algunas de las recomendaciones para el uso de las contraseñas tradicionales:

• Elija contraseñas que no se adivinen fácilmente. Muchos programas de detección automatizada de contraseñas utilizan un diccionario muy extenso y pueden descifrar contraseñas en cuestión de segundos.

• Cambie las contraseñas predeterminadas inmediatamente después de instalar equipos de infraestructura de red nuevo. Se deben cambiar las contraseñas para el acceso a la consola y las que se usan con fines de mantenimiento.

• Proporcione directrices sobre la frecuencia con la que usuario deber cambiar su contraseña. Conviene cambiar las contraseñas al menos cuando una cuenta con privilegios queda expuesta, o cuando haya un cambio critico en el personal.

¿Cómo elegir las contraseñas?

A continuación algunas directrices para elegirlas contraseñas apropiadas:

1. *No utilice el nombre de inicio de sesión arbitrariamente (tal como es, invertido, en mayúsculas, duplicado, etc.).*
2. *No utilice el nombre o el apellido arbitrariamente.*
3. *No utilice los nombres de parientes muy próximos o los nombres de personas o animales muy allegados. (esposa, esposo, novia, padre, mascotas, etc.).*
4. *No emplee otra información relativa a su persona o pertenencias que se obtenga de manera sencilla, como los números de matrícula del carro, los números de teléfono, la marca del carro que conduce, el nombre de la calle donde vive, etc.*
5. *No utilice una contraseña de todos dígitos o que tenga toda ella las mismas letras. Este tipo de contraseñas reduce el tiempo de búsqueda de un atacante.*
6. *No utilice una palabra que se incluya en los diccionarios de inglés, de español o cualquier idioma, listas ortográficas u otra lista de palabras.*
7. *No emplee una contraseña que tenga menos de seis caracteres.*
8. *No revele nunca su contraseña de red. La protección de la contraseña es su responsabilidad.*
9. *La finalidad última de que haya una contraseña consiste en asegurarse de que nadie (que no sea usted) pueda usar sus inicios de sesión. Recuerde que los secretos mejor guardados son los que se guardan para uno mismo.*
10. *No envíe por correo electrónico su contraseña.*
11. *Utilice siempre una contraseña que incluya caracteres no alfabéticos, como dígitos o signos de puntuación.*
12. *Utilice una contraseña que sea fácil de recordar, ya que conviene no anotarla.*
13. *Utilice una contraseña que pueda escribir rápidamente sin tener que mirar el teclado. Esto hará que sea más difícil que alguien se apropie de su contraseña.*
14. *Cuídese de escribir contraseñas delante de los demás.*
15. *Cambie su contraseña periódicamente. Trate de cambiarla cada tres meses.*

4. Normas y procedimientos para el personal

Las personas encargadas de mantener y actualizar la infraestructura de red deberán tener directrices específicas que les ayuden a desempeñar sus tareas con arreglo a las normas de seguridad corporativas.

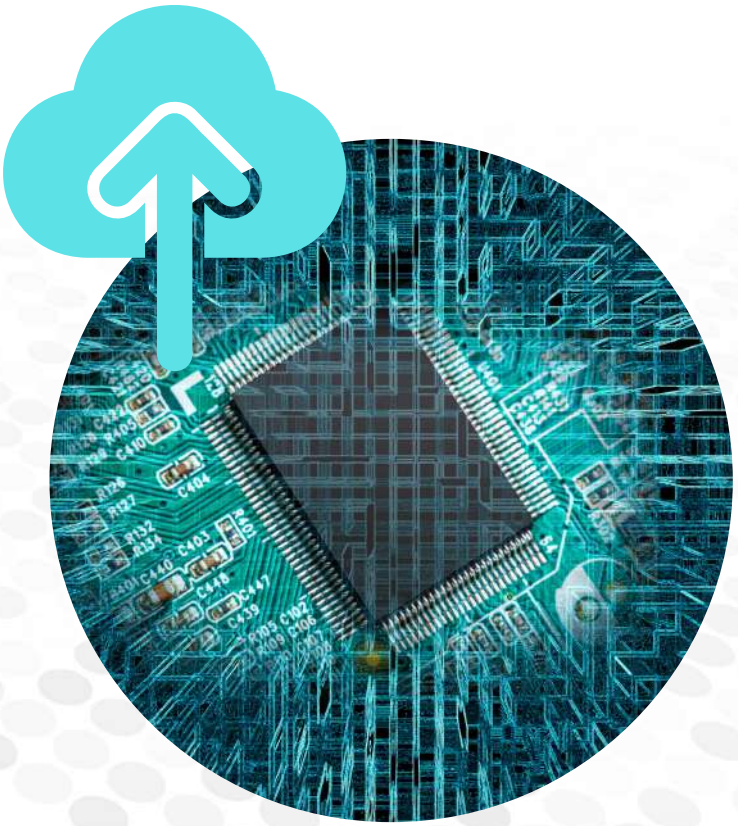
Copias de Seguridad

El procedimiento para la creación de copias de seguridad constituye una parte integral de la ejecución de un entorno computacional. La siguiente lista muestra las normas de copia de seguridad a seguir:

- Asegúrese de que su sitio está creando copias de seguridad para todas las configuraciones e imágenes de software del equipo de la infraestructura de red.
- Asegúrese de que su sitio está creando copias de seguridad para todos los servidores que proporcionen servicios de red.
- Asegúrese de que su sitio esta almacenando fuera del sitio las copias de seguridad. El sitio de almacenamiento deberá seleccionarse cuidadosamente en aras de la seguridad y disponibilidad.
- Cifre sus copias de seguridad para proporcionar una protección adicional a la información cuando esta fuera del sitio.
- No presuponga que las copias de seguridad siempre son buenas.
- De forma periódica, verifique el estado y la corrección de sus copias de seguridad.

Uso de equipos y herramientas portátiles

Los equipos portátiles plantean riesgos. Debe asegurarse de que el robo de alguno de los equipos portátiles de un miembro del personal no va a causar problemas. Se deben desarrollar directrices para los tipos de datos que residen en los discos duros de los portátiles, así como para la protección de los datos (por ejemplo si se debe utilizar o no el cifrado) cuando se trate de una computadora portátil.



5. ¿Qué es la ciberseguridad o seguridad cibernética?

La seguridad cibernética, el ataque cibernético, el crimen y el espionaje cibernéticos son palabras de moda conocidas en la prensa y en los redes sociales públicas como delitos que afectan estados, organizaciones y personas frecuentemente. Esto se debe en parte al desarrollo técnico, con el que avance la TI, pero se debe así mismo principalmente al continuo crecimiento del número de incidentes de seguridad, actos delictivos y nuevos métodos de ataque a la redes de información. El mito de que los hackers son personas con experiencia comprobada, ha dado paso a la comprensión que son en su mayoría organizaciones y grupos bien organizados con fines de lucro, los que están detrás de estos delitos.

En consecuencia, la ciberseguridad se está convirtiendo en una faceta cada vez más importante de la seguridad de la información y debe ser tenida en cuenta por la alta dirección de una organización; requiere como lo vimos al inicio de este documento, del uso de los recursos adecuados, gestionando el riesgo y debe ser una parte integral de todos los proceso para mitigar este riesgo en la empresa. La comprobación de los controles existentes en el marco de una verificación de seguridad cibernética, debe ser una labor diaria que permita garantizar un adecuado funcionamiento de los recursos TI y pueda protegerse a las organizaciones y las personas de ser víctimas de un ataque cibernético, delito cibernético o espionaje.

Ataques cibernéticos y amenazas persistentes avanzadas (APT - Advanced Persistent Threats) Por sus siglas en inglés.

Las organizaciones deben hacer frente a diario a las amenazas, los escenarios de riesgo y las vulnerabilidades relacionadas con TI. Ataques cibernéticos dirigidos por delincuentes con avanzados conocimientos y destrezas representan hoy desafíos, al estar bien organizados y equipados profesionalmente, configurando la más alta amenaza para empresas y organismos gubernamentales, así como para sus socios.

Este tipo de ataque a menudo se resume bajo el término APT (amenaza persistente avanzada) (ver [ISACA7]). Las APT suelen ser muy complejas tanto en preparación como en ejecución y suelen llevarse a cabo en varias fases. El objetivo de una APT, es pasar desapercibida mientras es posible espiar información confidencial o causar otros daños durante un período de tiempo más largo. Este tipo de ataque cibernético a menudo tiene antecedentes profesionales (por ejemplo, delitos cibernéticos o espionaje industrial), es difícil para detectar y los atacantes sólo se identifican con un esfuerzo considerable.

La siguiente figura muestra cómo se han desarrollado las amenazas a lo largo del tiempo y la motivación detrás de ellas.

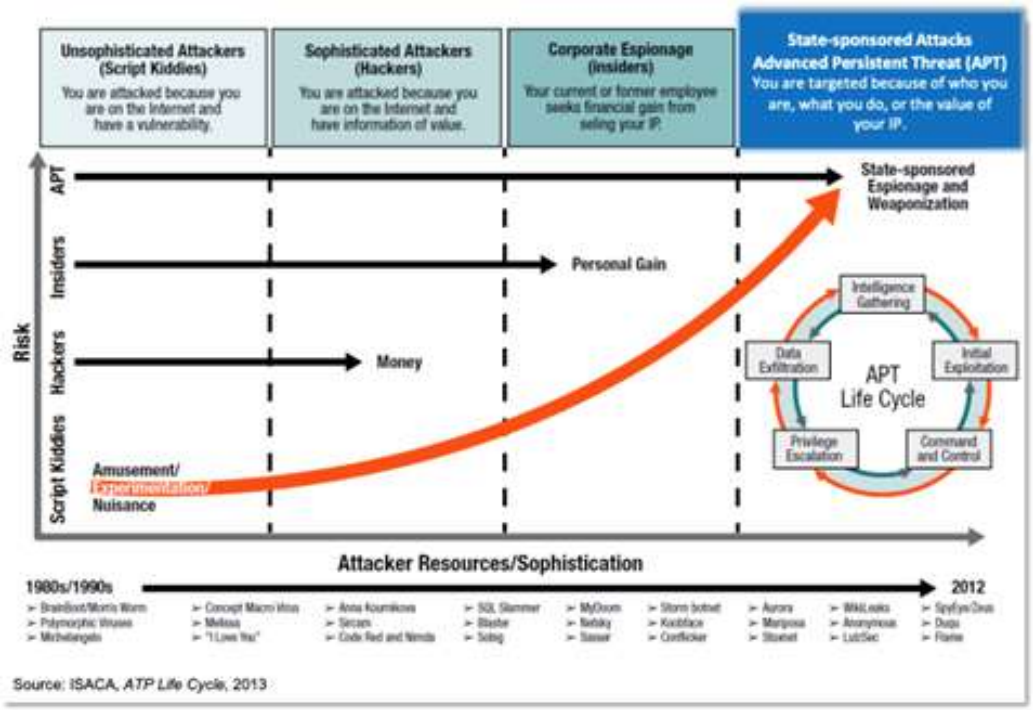


Figura N°4. Amenazas en ciberseguridad

- Señales de alerta para identificar amenazas de ciberseguridad.
- Principios básicos para implementar ciberseguridad.
- Implementación de un Chequeo de Seguridad Cibernética.

El riesgo de ser víctima de un ciberataque basado en APT no se puede excluir por completo, pero se puede minimizar en gran medida implementando un control de seguridad cibernética. Si una organización ya ha sido víctima de un ataque APT y/o si se sospecha de un ataque APT, se deben implementar controles adicionales más allá de los controles de seguridad cibernética.

Efectos del ciberdelito en las organizaciones y la sociedad

Hoy en día, las amenazas que plantean los delitos y el espionaje cibernético tienen numerosos efectos sobre la sociedad, las organizaciones y las personas afectadas. Para hacernos una idea desde cuando se tiene trazabilidad de estos delitos podríamos citar el año 2006, donde el crimen organizado como el gobierno y las agencias de seguridad, presenciaron distintos hechos y visibilizaron que los ataques cibernéticos podrían instaurarse en el orden mundial. A continuación los resultados que se incluyeron desde esta fecha:

- *Robo de información confidencial, datos de productos y desarrollos hasta el espionaje sistemático.*
- *Robo de propiedad intelectual, manipulación de transacciones comerciales, malversación de fondos.*
- *Fraude financiero, uso indebido de tarjetas de crédito, falsificación y uso indebido de identidades.*
- *Sabotaje de procesos de negocio a través de ciberataques destructivos y ataques de denegación de servicio.*

El cibercrimen, como todo el campo de la tecnología de la información, es muy dinámico. A la lectura de este documento podrá usted seguir consultando y el crecimiento de los índices va en aumento. Si bien las cifras de delitos en muchas áreas han mejorado la contingencia, los delitos cibernéticos en el sentido estricto del término está aumentando continuamente.

Las estadísticas del crimen en mención de la Oficina Federal de Policía Criminal (BKA), datan por ejemplo: en el 2017 se registró un total de 85.960 delitos. Esto representó un aumento de 4% interanual registrado en el (2016: 82.649). Al evaluar tales cifras de casos, debe tenerse en cuenta que cada hecho ilícito, independientemente del número de víctimas, se registra como un solo caso. Por ejemplo, en noviembre de 2016 el programa manipulación es de aproximadamente 1,3 millones de enrutadores DSL de un proveedor alemán de Internet por malware (Mirai), a pesar de este número de siete dígitos de víctimas – se registró como solo una instancia de Sabotaje informático en el informe estadístico de la Policía Criminal Federal Oficina (ver [BKA17]).

Además, de las cifras anteriores se supone que existe un elevado número de casos no declarados. Casos, que nunca aparecen en las estadísticas: según una encuesta de la BSI, El 70 % de las empresas alemanas entrevistadas se vieron afectadas por ciber ataques en 2017. La mayoría de estos ataques (57%) fueron ejecutados por medio de malware. Esta evaluación de la situación de amenaza está respaldada por el informe sobre el estado de la seguridad informática del BSI para 2019.

Con este contexto internacional puede usted como empresario considerar o no el ciberdelito como un factor a considerar.

6. Principios básicos de ciberseguridad

Mediante la implementación de un control de seguridad cibernética, las empresas y agencias gubernamentales pueden determinar el nivel actual de seguridad cibernética de sus organizaciones. Como se sabe de la seguridad de la información, dicha evaluación debe llevarse a cabo sobre la base de un marco integral a fin de proporcionar declaraciones fundamentadas. Esta guía y el control subyacente de objetivos para la evaluación, se basan en el concepto probado de tres líneas de defensa, que se centran por completo en los aspectos de seguridad cibernética.

Esta figura ejemplifica tales aspectos relevantes para la seguridad cibernética para las líneas respectivas de defensa.

- Controles internos
- Cumplimiento de la seguridad cibernética
- Aceptación formal del riesgo

- Amenazas, vulnerabilidades, riesgos
- Análisis de riesgo formal
- Análisis de impacto empresarial (BIA)
- Autoevaluación / evaluación

- Pruebas funcionales y técnicas
- Revisión periódica de la gestión

Figura N° 5 el concepto de las tres líneas de defensa
Fuente: SICK AG, línea de defensa, Teuscher A., enero de 2019

1

La primera línea de defensa, la gerencia ejecutiva/superior de una organización, primero debe comprender la necesidad de los controles de seguridad cibernética, los requisitos de protección de los procesos de negocio así como sus dependencias y amenazas.

2

La segunda línea de defensa, es la gestión de riesgos y seguridad que debe analizar la medida en que los riesgos de ciberseguridad afectan a la organización y a sus procesos y qué controles podrían implementarse para prevenir esto. La función de gestión de riesgos de la organización es el primer organismo independiente en revisar y evaluar las decisiones del ejecutivo/alta dirección, aunque sin poder decisorio propio. La decisión final sobre la implementación de controles de seguridad queda en manos del ejecutivo/ Gerencia senior.

3

La tercera línea de defensa, es la auditoría interna o externa, por ejemplo, por auditoría informática. Aquí es donde entra en juego el control de ciberseguridad, con que una evaluación independiente y objetiva del nivel existente puede hacer seguridad. El evaluador apoya a la organización en el logro de sus objetivos utilizando un enfoque sistemático y enfocado para evaluar la seguridad cibernética en la organización y promoviendo la optimización de la seguridad, evaluando controles a través de sus actividades y auditoría.

Para generar confianza en una evaluación objetiva, tanto los particulares como las empresas deben cumplir los siguientes requisitos previos prestación de servicios en el ámbito de la ciberseguridad:

a. Mandato formal para el control de ciberseguridad por parte de la organización.

(ver Estándar BASC para implementación del estándar, u otro estándar internacional de SI

b. Integridad y confidencialidad (consulte procedimiento de auditoría BASC– Debido Cuidado Profesional [ISACA6])

c. Experiencia profesional (para Auditoría y Garantía – Competencia

d. Evidencia y trazabilidad (ver Auditoría y Aseguramiento de SI)

e. Objetividad y diligencia (consulte los Estándares de auditoría)

f. Presentación objetiva y fáctica (ver Estándar BASC para SI en Auditoría y Aseguramiento)

7. Ingeniería social

Muchos intrusos tienen más éxito utilizando la ingeniería social que la piratería técnica. Una de las normas de formación más importantes es que los empleados y los usuarios no deben creerle a cualquiera que llame por teléfono y les pregunte por algo que pueda poner en peligro la seguridad. ¿Por qué revelar al interlocutor información financiera personal y aceptar una nueva contraseña por teléfono? Esto no puede ser así, ya que no se ha establecido la identidad del interlocutor. Lo mismo es aplicable a las contraseñas y a la información corporativa confidencial solicitada por teléfono. Antes de divulgar información confidencial, deberá identificar positivamente a la persona con la que se está hablando.

8. Conclusiones

Para ser eficaces, los procedimientos de seguridad informática deberán ser concisos e ir al grano. Deberán abarcar reglas que definan los controles de seguridad física (que pertenecen a la infraestructura física, a la seguridad de los dispositivos físicos y al acceso físico). Entre estas reglas se deberán incluir directrices que protejan la integridad y confidencialidad de los datos con el fin de garantizar que tales datos no han sido alterados durante el tránsito y que solo son entendibles por el emisor y el destinatario de la información. También resulta imperativo que las empresas proporcionen a los empleados una formación apropiada y que les instruyan acerca de los potenciales problemas relacionados con la seguridad informática.

BASC Colombia
Colaboradores

Autor:

Ramiro Humberto Nova Jaimes

Psicólogo de la Universidad Autónoma de Bucaramanga UNAB. Especialista en alta Gerencia. Doctor en Ciencias Mención Gerencia. Estancia postdoctoral Universitario Tecnológico Terra At Mundi Universitam. Posdoctorado en Administración y Finanzas. Diplomado en Logística Internacional- BASC Colombia y SENA. Auditor Internacional BASC- WBO desde el año 2004, con más de 90 auditorías. al sector Transportador terrestre, sector Vigilancia y Seguridad Privada, sector Exportador, sector Operador Logístico, Sector Agente de Aduana, Sector portuario y sus servicios. Auditor en Sistemas Integrados de Gestión normas ISO 9001, ISO 14001, OHSAS 18001, RUC. ISO 45001:2018. Formador de formadores desde el año 2013. (Para la formación de auditores internos BASC).

Comisión de expertos:

Wilson Yecid Triana Roa:

Master en Gestión de Riesgos, Especialista en Gerencia de la Calidad y Economista. Auditor Internacional BASC - Sistema de Gestión en Control y Seguridad y Auditor Líder ISO 28000. Experiencia en consultoría e implementación de esquemas de seguridad en las instalaciones, bienes, personas y operaciones logísticas de organizaciones que participan en comercio exterior mediante la aplicación de prácticas de seguridad y gestión del programa OEA y sistema de gestión en control y seguridad BASC para las cadenas de suministros. Orientación en la gestión de riesgos para la continuidad de negocio en las organizaciones y protección de bienes, personas, instalaciones y cadena de suministros.

Propiedad del documento:
BASC Colombia
Luis Bernardo Benjumea Martínez
Director Ejecutivo

Comité BASC encargado - Centro de información y pensamiento, integrado por:

Silvia Carolina Sánchez Monsalve
Directora Ejecutiva
BASC Oriente

María Carolina Vives Noriega
Directora Ejecutiva
BASC Santa Marta

Lilibeth García Lora
Coordinadora Administrativa
BASC Santa Marta

Luisa María Vega Andrade.
Asistente Administrativa
BASC Colombia

Diseño y producción de la cartilla:

Pía Margarita Sierra Sánchez
Coordinadora de Capacitaciones y Comunicaciones
BASC Oriente

Revisado y publicado, junio de 2022

BUSINESS ALLIANCE FOR SECURE COMMERCE

B A S C C o l o m b i a

Antioquia - Barranquilla - Bogotá - Café - Caldas - Cartagena -
Centro Occidente - Oriente - Santa Marta - Sur Occidente