12 MARZO 2021

II CONGRESO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

“Gobierno y Gestión de la Ciberseguridad”

SOCHISI
DIGITAL SECURITY THINK TANK

HACKADA

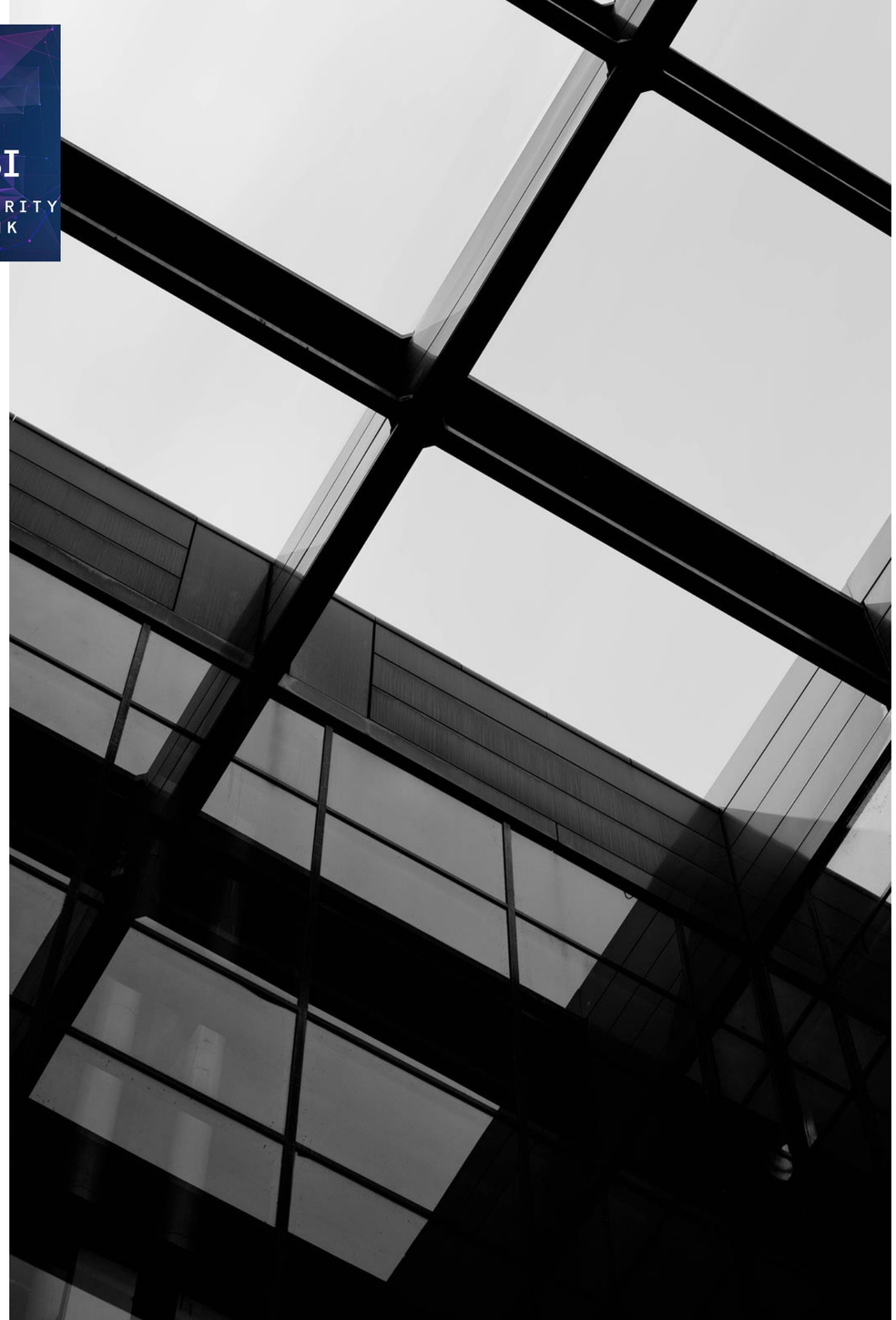
Speakers:

Mg. Bárbara Palacios Cabezas
Ing. Constanza Herrera Pizzoleo

Linkedin

https://cl.linkedin.com/in/bpalaciosc
https://www.linkedin.com/in/ConstanzaHerreraPizzoleo

SOCHISI.CL/ENVIVO



¡Bienvenid@s a la nuestra charla!

Agenda de hoy

01 Expositoras.

02 ¿Qué es la gestion de la Ciberseguridad?

03 Seguridad de la Información y Ciberseguridad.

04 Gestión de activos de información

05 Gestión de riesgos.

06 Gestión de incidentes.

07 Gestión del cumplimiento.

08 Gestión de la continuidad del negocio.

09 Gestión de la cultura en Ciberseguridad.

SOCHISI.CL/ENVIVO

Objetivos y reglas de la charla

Expectativas y resultados

Objetivos

Dentro de los objetivos de esta charla Podemos encontrar:

- Poder ser capaces de identificar en que se diferencian Ciberseguridad y Seguridad de la Información, y, a su vez, que tienen en común.
- Explicar en que consiste el Gobierno de Ciberseguridad y cómo gestionarlo.
- Explicar como gestionar la Ciberseguridad, dando el enfoque de un estándar bajo los framework que apoyan.
- Concientizar sobre la cultura en la Organización sobre Ciberseguridad y Seguridad de la Información.

Reglas

Aquí no existen reglas, salvo el estar dispuesto a aprender.

Seguridad de la Información VS Ciberseguridad

- ¿Seguridad de la información o Ciberseguridad?
- ¿De qué se trata cada una?
- ¿Qué es la gorbernanza?
- ¿Cómo se gestiona la Ciberseguridad?

Hablaremos de eso y mucho más aquí...

Mg. Bárbara Palacios Cabezas

https://cl.linkedin.com/in/bpalaciosc

barbara.palacios@usach.cl

Oficial de Ciberseguridad de la Contraloría General de la República, con 7 años de experiencia profesional en Seguridad de la Información en sector consultoría, sector financiero y banca. Magíster en Seguridad, Auditoría y Peritaje, y Analista y Computación Científica de la Universidad de Santiago de Chile, Diplomado en Ciberseguridad de la Universidad de Chile. Certificada CISA (ISACA), en Hacking Ético y Pentesting (CHP), Auditor Líder 27001, Gobierno y Gestión de Ciberseguridad usando COBIT por la Universidad de Santiago de Chile, Lead Cybersecurity Professional (LCSPC) y Cyber Security Foundation (CSFPC) de CertiProf.

Forma parte de la Sociedad Chilena de la Seguridad de la Información (SOCHISI), Level[0]Sec, HackAda (Mujeres en Ciberseguridad), PartyHack, WOMCY y Latin HTB.

Ing. Constanza Herrera Pizzoleo

https://www.linkedin.com/in/ConstanzaHerreraPizzoleo

conytaherrera@usach.cl

Ingeniero en Informática, Diplomado en Evaluación Integrada de Proyectos y en proceso de finalización del Diplomado en Gobernanza, Gestión y Auditoría a la Ciberseguridad, con más de 10 años de carrera profesional, y al menos 5 dedicados a la Gestión de Proyectos, actualmente se desempeña como Jefe de Proyectos de Ciberseguridad en Banco Itaú.

Forma parte de la Sociedad Chilena de la Seguridad de la Información (SOCHISI), Level[0]Sec y HackAda (Mujeres en Ciberseguridad).

Posee distintas certificaciones, como Lead Cybersecurity Professional Certificate (LCSPC), Auditor ISO 27001, Cyber Risk and Internal Auditor, ITIL v3, y Scrum Máster, entre otras.

Antes de comenzar, algunos conceptos...

Seguridad de la Información

Es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información, buscando siempre mantener la confidencialidad, integridad y disponibilidad de los datos, respecto a distintas amenazas, tales como pérdidas de datos personales, registros financieros, entre otros.

Ciberseguridad

Es la protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, se almacena y se transporta mediante los sistemas de información que se encuentran interconectados

Gestión

Conjunto de operaciones que se realizan para dirigir y administrar un negocio o una empresa.

Gobierno de Seguridad de la Información

- El gobierno de seguridad de la información consiste en el liderazgo, estructura organizacional y proceso para proteger la información.

- El gobierno de seguridad de la información es un subconjunto del gobierno corporativo de la organización que provee dirección estratégica, garantiza los objetivos establecidos, gestiona los riesgos de forma apropiada, usa los recursos organizacionales responsablemente y monitorea el éxito o falla del programa de seguridad de la organización.

Gobierno de Ciberseguridad

El gobierno de ciberseguridad es una estrategia basada en el conocimiento y en la organización en base a:

- **Análisis de riesgos:** identificar los componentes de riesgos de los sistemas TIC con respecto a los procesos de negocio.

- **Plan director de seguridad:** integración delos procesos del área de seguridad informática en un único sistema de gestión.

¿Qué es la Gestión de la Ciberseguridad?

El objetivo de gestionar la ciberseguridad es reducir los riesgos en este ámbito hasta un nivel aceptable para los interesados y, por lo tanto, debe incluir todas aquellas actividades tendientes a implantar las medidas de protección adecuadas. Se gestionan los riesgos, actividades, necesidades y acciones asociadas a la ciberseguridad, con el fin de reducir las brechas al mínimo posible, manteniendo la operación de la organización.

Seguridad de la Información y Ciberseguridad

¿Qué entendemos por Seguridad de la Información?

Por seguridad de la información se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. Dicho de otro modo, son todas aquellas políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización.

.

¿Seguridad de la Información o Ciberseguridad?

Esto siempre dependerá del punto de vista que se esté revisando. Se debe destacar que la Ciberseguridad es un subconjunto de la Seguridad de la Información.

ISO 27.001 / ISO 27.002

- Define lineamientos y controles de seguridad de la información
- Vela por la confidencialidad, integridad y disponibilidad de la información.
- Crea y define un Sistema de Gestión de Seguridad de la Información (SGSI).
- Basada en riesgos.

ISO 27.032

- Define las guías para la ciberseguridad.
- Cubre las brechas que no han sido abarcadas en normas anteriores, considerando el ámbito conceptual más amplio (Ciberespacio), donde aparecer nuevos desafíos de Ciberseguridad y también, de seguridad de la Información.
- Cubre el proceso de colaboración entre todos los actores que operan en el entorno. (CSF – Cybersecurity Framewok)

Seguridad de la Información y Ciberseguridad

Seguridad de la Información y Ciberseguridad

Gestión de activos de información

Gestión de activos

¿Qué es la gestión de activos?

La gestión de activos de información involucra el diseño, establecimiento e implementación de un proceso que permita la identificación, valoración, clasificación de los activos de información más importantes para la institución.

De acuerdo con la **NCH ISO 27001: 2013**, un activo de información es “algo que una organización valora y, por lo tanto, se debe proteger”.

Se puede considerar como un activo de información a lo siguiente:

- Los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios.
- El hardware y el software utilizado para el procesamiento, transporte o almacenamiento de información.
- Los servicios utilizados para la transmisión, recepción y control de la información.
- Las herramientas o utilidades para el desarrollo y soporte de los sistemas de información.
- Personas que manejen datos, o un conocimiento específico muy importante para la organización. Por ejemplo: secretos industriales, manejo de información crítica.

- Esta tarea está a cargo de las gerencias de seguridad o de gestión de la información, que involucra el diseño, establecimiento e implementación de un proceso que permita la identificación, valoración, clasificación y tratamiento de los activos de información más importantes del negocio.
- Responden a la Triada de Seguridad (Confidencialidad, Integridad y Disponibilidad)
- Se clasifican según su Prioridad (Alta, Media, Baja)
- Se pueden considerar dos tipos Tangibles e Intangibles.
- Asociados a la ISO 27001, incluidos el anexo A.

Activo de información intangible

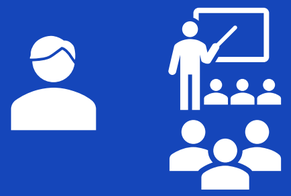
Ejemplo

Supongamos que Tomita está a cargo de mantener el listado de usuarios, la que maneja en una Planilla de Excel

¿Qué riesgos corre Tomita?

- Fuga de información
- Integridad de datos
- Pérdida de información confidencial
- Incluso, sufrir un ataque de Malware que comprometa esta información.

Entre otros...



Ejemplo

Tomita es consciente de estos riesgos, por lo que decide hablar con su supervisor y le indica éstos, comentándole que lo que debería realizar la Organización es mantener esta información sensible no en una planilla, sino que en una BD como AD, por ejemplo, además, comenta que es importante manejar los accesos a través de una bóveda, y designar a un custodio que se comprometa a guardar y proteger la información.

Ejemplo

Tomita ahora cuenta con una bóveda que administra las cuentas, sobre todo las de altos privilegios, además, generó en conjunto con su equipo una política de control de cuentas, todas las cuentas de la Organización se trabajan en un AD, que se conecta a los servidores que sostienen la bóveda, se rige bajo políticas e incluso normativas, y logró minimizar los riesgos asociados.

Activo de información tangible

Ejemplo

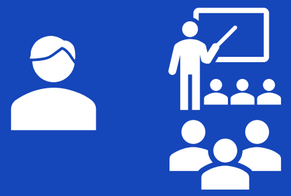
Tomita ahora está a cargo de un laboratorio de computación de una institución educacional, este laboratorio está cerca de los baños del piso.

¿Qué riesgos corre Tomita?

Que ocurra un derrame de agua en el piso que pueda afectar a la parte eléctrica del laboratorio

Que no tenga respaldo de la información

Que entre un malware en la red.



Ejemplo

Tomita toma conciencia de estos riesgos, por lo que decide hablar, tanto con el prevencionista de riesgos de la institución, como con el encargado de informática y redes, expone la situación, por lo que el prevencionista decide evaluar los riesgos y entregar un informe detallado de éstos.

El encargado de informática y redes, toma conciencia y decide comenzar a evaluar soluciones de backup, HA, antivirus, y también, segmentación de red.

Ejemplo

Tomita ahora cuenta con una política de respaldos, además de que la red del laboratorio se encuentra separada de la red Organizacional, evitando así, un ingreso de Malware que podría afectar a ésta, cuenta también, con un Playbook que le ayudará a saber como actuar ante distintas situaciones.

Finalmente, la organización también cuenta con políticas de prevención de riesgos físicos y del entorno, señaliza los accesos y también, se sabe como actuar antes distintos incidentes relacionados

Gestión de activos

¿Cómo los abordamos?

- Manteniendo un catastro de todos los activos físicos y también lógicos de la Organización.
- Revisiones y mantenciones programadas con la frecuencia que se decidió en comité (mensual, trimestral, semestral, anual, etc.).
- Actualizaciones de sistema al día (parches S.O, KB, actualizaciones de Software, etc.).
- Mantener sistemas que protejan tanto los endpoints como los alojados dentro de la DMZ (AV, EDR, DLP, IPS, Anti DDoS, etc.).
- Mantener las políticas siempre actualizadas, con revisiones periódicas y asociados a la realidad de la Organización.
- Asegurar no solo la Seguridad en el Ciberespacio, sino que también la Seguridad física y del entorno (cámaras, accesos físicos, locaciones, mantenciones de las ubicaciones físicas, eléctricas, contar con un prevencionista que esté revisando constantemente los riesgos del entorno).

Gestión de Riesgos

¿Cómo gestionamos los riesgos?

¿Qué es la gestion de riesgos?

Es la acción preventiva de cualquier evento que pudiese generar una indisponibilidad o ataque en la Organización, asociado a Ciberseguridad, sería la acción preventiva para identificar, contener y/o prevenir cualquier evento que pudiese afectar a la continuidad operativa de la Organización.

Se define por la siguiente fórmula:

Riesgo = **Intención** x **Vulnerabilidad** x **Consecuencia**

En donde:

- **Intención:** es la capacidad del atacante en base al nivel de sofisticación y recursos. (opcional)
- **Vulnerabilidad:** es la brecha que permite un ataque, está presente y es explotable para producir un impacto material.
- **Consecuencia:** es el valor económico del activo o activos en riesgo.

¿Cuáles serían riesgos en Ciberseguridad y Seguridad de la Información?

Tipos de Riesgos de Ciberseguridad y Seg. de la Información

- **Riesgo residual:** Riesgo remanente que existe después de que se hayan tomado las medidas de seguridad.
- **Riesgo de aceptación:** Decisión informada para tomar un riesgo en particular.
- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo.
- **Evaluación de riesgos:** Proceso general de identificación, análisis y evaluación de riesgos.
- **Estimación de riesgos:** Proceso de comparación de los resultados del análisis de riesgos con los criterios de riesgos para determinar si el riesgo y/o su magnitud son aceptables o tolerables.
- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización respecto al riesgo.
- **Tratamiento de riesgos:** Proceso para modificar el riesgo.

Ataques y/ Riesgos más comunes
1. Malware
2. Ataques a la red
3. phishing
4. Fuga de Información
5. hishing o usurpación de identidad
6. Amenazas a entidades bancarias
7. Riesgo reputacional
8. Ataques DDoS
9. Ransomware
10. Botnets
11. Inyección SQL

¿Cuáles serían riesgos en Ciberseguridad y Seguridad de la Información?

Ejemplo

- BYOD
  - Actualmente las barreras de las comunicaciones y el teletrabajo permiten tener “ciertos” tipos de licencias, como por ejemplo, un estudio sobre trabajadores de oficina según el cual el 75 % realiza tareas personales en el tiempo de trabajo y el 77 % realiza tareas relacionadas con su trabajo en su tiempo personal, considerando que la gran mayoría de estas actividades se hacen a través de los Smartphone, y que muchas veces, utilizamos el mismo dispositivo tanto para trabajo, como para temas personales.
  - Muchas veces el dispositivo que se utiliza es el de uso personal del usuario. (independiente de las medidas que tomen las empresas anti – BYOD) – Fortinet 2012
- BYOA
  - Bajo el mismo escenario del BYOD, existe el BYOA (Bring yoour own application), el cual indica que los usuarios utilizan sus propias app (descargadas en los Smartphone) dentro del horario laboral.
  - Aproximadmente un 70% de las empresas estaba conciente de este riesgo (Estudio Telefónica – 2016)

Pero, ¿Cuáles son los Beneficios que se identifican en el uso de BYOD y BYOA?.

- Accesibilidad.
- Conveniencia y flexibilidad.
- Satisfacción del empleado.
- Incremento de la productividad y de la innovación.
- Reducción de costes.

¿Cuáles serían riesgos en Ciberseguridad y Seguridad de la Información?

BYOD y BYOA – Necesidades de Seguridad

- Generar nuevo proceso y/o procedimientos que sean capaces de cubrir las necesidades de Seguridad de la Organización
- Considerar que puede existir Fuga de Datos
- Considerar que al ser un OD u OA, pueden existir conflictos asociados a Privacidad.
- Al ser un dispositivo que no está bajo una imagen aprobada por la organización o bajo las reglas de ésta, puede estar más expuesta a ciberataques.
- Considerar que si el dispositivo se conecta a la red corporativa, es más fácil poder acceder a recursos que son sensibles.
- Existe el riesgo de robo o de pérdida del dispositivo.

¿Y cómo podemos gestionar éstos?

- Considerando siempre la existencia del riesgo
- Tomando el riesgo como parte de la organización
- Siendo capaces de poder identificarlos, poder analizarlo, y poder plasmar éstos en conjunto con controles que pueden ayudar en la mitigación.
- Poniendo nota al riesgo, según el valor que tiene para la Organización.
- Indicando prioridad del riesgo, según la experiencia y nivel de complejidad.
- Generando una matriz que contenga toda esta información, además de otra información que sea relevante para la organización. (CONOCER EL NEGOCIO).
- Tomar las lecciones aprendidas, hacerlas parte del día a día.
- Generar una CMDB

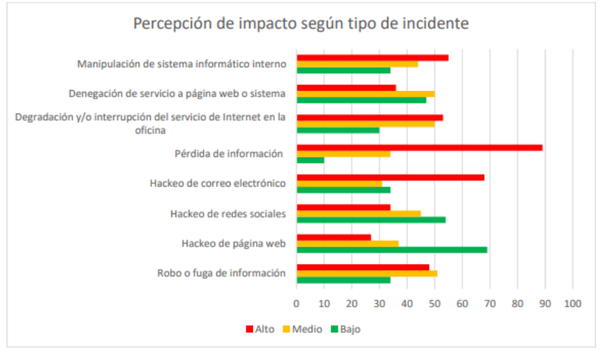
Matriz de Riesgos

¿Cómo generamos la Matriz de Riesgos?

- Identificar todos aquellos activos de información que tienen algún valor para la organización.
- Asociar las amenazas relevantes con los activos identificados.
- Determinar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.
- Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

		Probabilidad		
		Baja	Media	Alta
Impacto	Alta			
	Media			
	Baja			

Criticidad
Baja
Media
Alta



Activo	Dimensión	Amenaza	Tipo	Posibles ataques	Probabilidad	Impacto	Criticidad	Control
Archivos almacenados en equipos de usuarios (computadoras o teléfonos)	Confidencialidad	Una persona desea obtener información sensible y/o de valor de la empresa, ya sea para aprovechar dicho conocimiento o para divulgarlo.	Externo	Implantación de un software malicioso que permita la filtración de archivos; vector de ataque ingeniería social Acceso físico al equipo que contiene los archivos	Baja; es muy poco probable que una PYME tenga un enemigo con los recursos e intención específica para exfiltrar información, cuyo valor es relativamente limitado	Alto; las PYMEs suelen almacenar toda la información del negocio en archivos, incluida información personal sensible de clientes	Media	Cifrado de archivos sensibles
			Interno	Acceso indebido a un equipo de la empresa al que no debería tener acceso. Copia no autorizada de archivos a los que tiene acceso	Media; podría haber pocas personas que tuvieran la intención de robar información de sus empresas, pero tendrán fácilmente la oportunidad y los recursos para hacerlo.	Alto; las PYMEs suelen almacenar toda la información del negocio en archivos, incluida información personal sensible de clientes	Alta	Contraseña de inicio de sesión y bloqueo de pantalla con contraseña (robustas y diferentes) en todos los equipos. Cifrado de archivos sensibles. Distribución granular de permisos para accesos a archivos
	Disponibilidad / Integridad	Alguien borra o inutiliza un archivo	Externo o Interno	Una infección por ransomware. Acción no intencional de un empleado o persona interna. Falla de un componente físico (ej.: disco duro)	Alta; los ataques de ransomware son uno de los más frecuentes, son fáciles de llevar a cabo, los eventos fortuitos son frecuentes	Alto; las PYMEs suelen almacenar toda la información del negocio en archivos	Alta	Copia de seguridad de archivos
	Integridad	Una persona modifica el contenido de un archivo con el objetivo de boicotear a la empresa u obtener un beneficio personal	Externo	Implantación de un software malicioso que permita la manipulación de archivos; vector de ataque ingeniería social	Baja; es muy poco probable que una PYME tenga un enemigo con los recursos e intención específica para modificar información	Alto; dependiendo de la criticidad del proceso asociada al archivo, su modificación podría tener graves consecuencias (cambios en un historial médico, cambios en un archivo contable, etc.)	Media	Cifrado de archivos sensibles
			Interno	Manipulación de un archivo al que tiene acceso	Media; podría haber pocas personas que tuvieran la intención de robar información de sus empresas, pero tendrán fácilmente la oportunidad y los recursos para hacerlo.	Alto; dependiendo de la criticidad del proceso asociada al archivo, su modificación podría tener graves consecuencias (cambios en un historial médico, cambios en un archivo contable, etc.)	Alta	Separación de roles - Generación de información y verificación de la información sensible antes de su uso

Gestión de Riesgos y el framework de ciberseguridad NIST

¿Qué es NIST?

Descubriendo el framework

Este marco ayuda a las empresas de todos los tamaños a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos. Les proporciona un lenguaje común y un resumen de las mejores prácticas en ciberseguridad.

Este marco no provee nuevas funciones o categorías de ciberseguridad, sino recopila las mejores prácticas (ISO, ITU, CIS,, entre otros) y las agrupa según afinidad. Se centra en el uso de impulsores de negocio para guiar las actividades de ciberseguridad y considerar los riesgos cibernéticos como parte de los procesos de gestión de riesgos de la organización. El framework consta de tres partes: el marco básico, el perfil del marco y los niveles de implementación.

Sobre el framework...

Marco básico (framework core)

Es un subconjunto de actividades de ciberseguridad, resultados esperados y referencias aplicables que son comunes a los sectores de infraestructuras críticas, en términos de estándares de la industria, directrices y prácticas que permiten la comunicación de actividades de ciberseguridad y sus resultados a lo largo de la organización, desde el nivel ejecutivo hasta el de implementación/operación. Consta de cinco funciones continuas que veremos en detalle

Niveles de implementación del marco

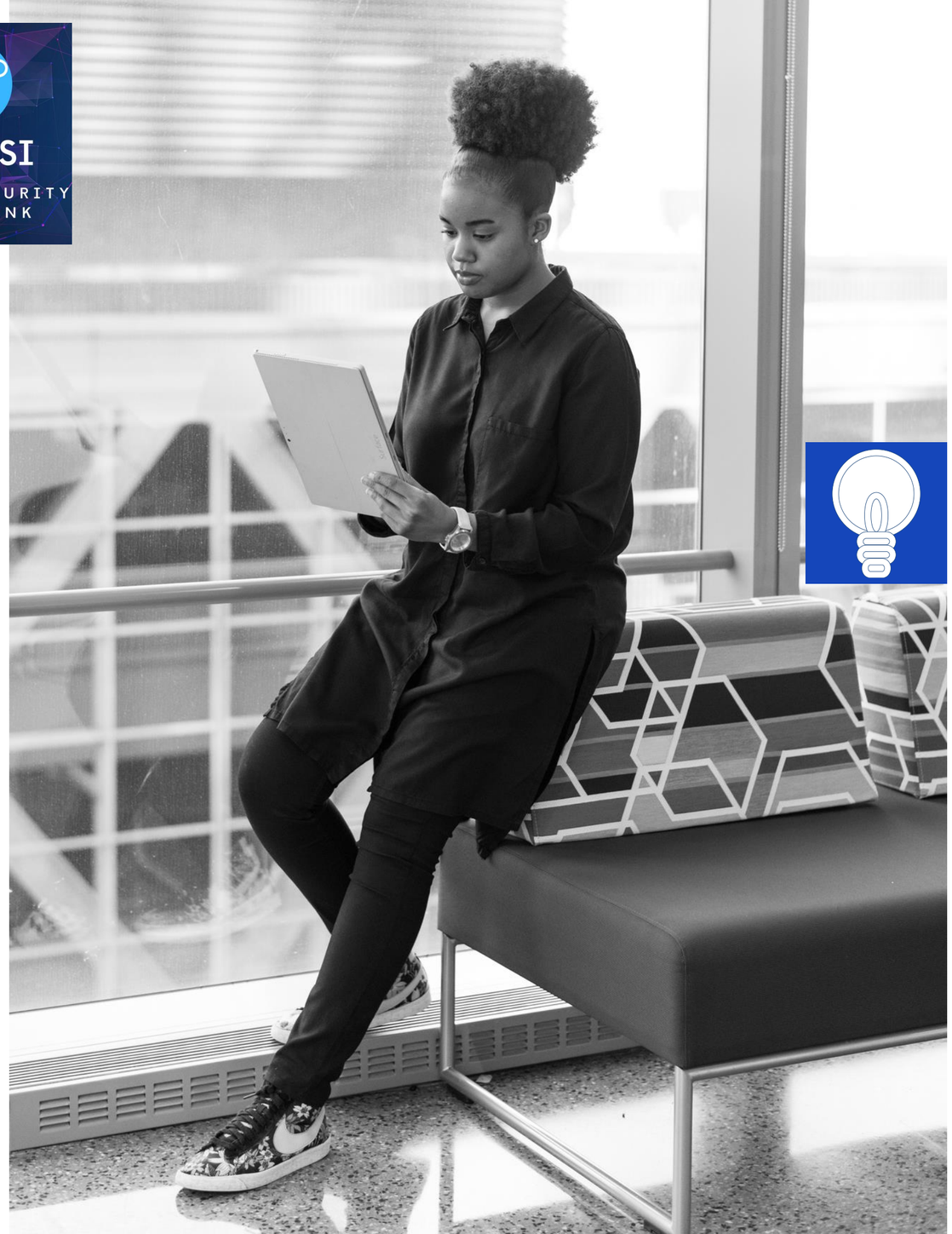
Los niveles de implementación le permiten a la Organización poder catalogarse en un umbral predefinido en función de las prácticas actuales de gestión de riesgo, el entorno de amenazas, los requerimientos legales y regulatorios, los objetivos y la misión del negocio y las restricciones de la propia empresa.

Perfiles del marco

Los perfiles se usan para describir el estado actual (perfil actual) y el estado objetivo (perfil objetivo) de determinadas actividades de ciberseguridad. El análisis diferencial entre perfiles permite la identificación de brechas que deberían ser gestionadas para cumplir con los objetivos de gestión de riesgos.

.

SOCHISI
DIGITAL SECURITY THINK TANK



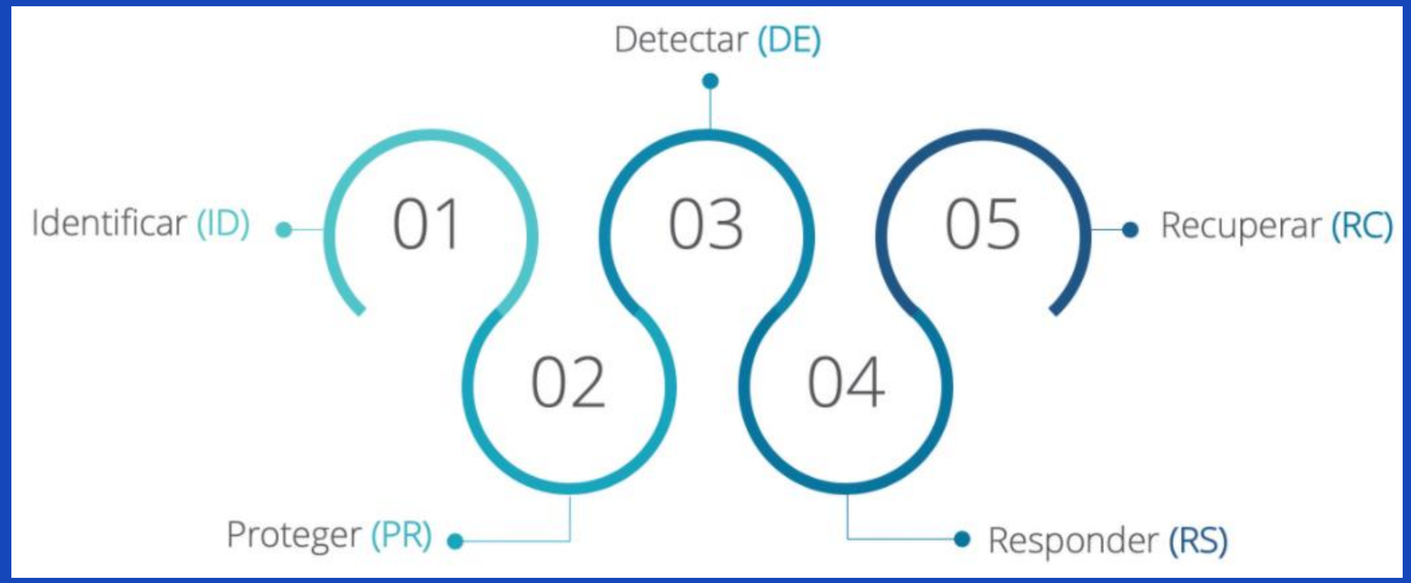
Entonces, ¿en qué consiste el framework?

NIST
National Institute of
Standards and Technology

El Framework Core (núcleo) comprende un conjunto de actividades de ciberseguridad, resultados y referencias informativas que son comunes a través de los sectores de infraestructura crítica. Así, proporciona la orientación detallada para el desarrollo de perfiles individuales de la compañía. Mediante el uso de los perfiles, el marco ayudará a la organización a alinear sus actividades de ciberseguridad con sus requisitos de negocio, tolerancias de riesgo y recursos. Por su parte, los niveles de implementación del marco (tiers) proporcionan un mecanismo para que las empresas puedan ver y comprender las características de su enfoque para la gestión del riesgo de ciberseguridad.

El núcleo del framework

Funciones del núcleo



El núcleo proporciona cinco funciones continuas. Asimismo, también brinda un conjunto de actividades para lograr resultados específicos de ciberseguridad y hace referencia a ejemplos de orientación para lograr esos resultados. El núcleo no es una lista de comprobación de las acciones a realizar. Presenta los resultados clave de ciberseguridad identificados por la industria como útiles para gestionar el riesgo cibernético. Comprende cuatro elementos: funciones, categorías, subcategorías y referencias informativas.

Funciones del núcleo

IDENTIFICAR	PROTEGER	DETECTAR	RESPONDER	RECUPERAR
CATEGORÍAS				
Gestión activos.	Control de concientización.	Anomalías y eventos.	Planes de respuesta.	Planes de recuperación.
Ambiente de negocios.	Concientización y entrenamiento.	Monitoreo contínuo de seguridad.	Comunicaciones.	Comunicaciones.
Gobernancia.	Seguridad de datos.	Procesos de detección.	Análisis.	Mejoras.
Evaluación de riesgos.	Protección de información y procedimientos.		Mitigación.	
Estrategia de gestion de riesgos.			Mejoras.	


Las funciones
Las categorías
Las subcategorías
Referencias informativas
organizan las actividades básicas de ciberseguridad en su nivel más alto. Estas funciones son Identificar, Proteger, Detectar, Responder y Recuperar.
son subdivisiones de una función en grupos. Ejemplos de categorías incluyen "Gestión de activos", "Control de acceso" y "Procesos de detección".
Dividen aún más una categoría en resultados específicos. Los ejemplos de subcategorías incluyen "Los sistemas de información externos están catalogados", "Los datos en reposo están protegidos" y "Se investigan las notificaciones de los sistemas de detección".
son secciones específicas de normas, directrices y prácticas comunes entre los sectores de infraestructura crítica que ilustran un método para lograr los resultados asociados con cada subcategoría.

Categorías de función e identificadores únicos

FUNCIÓN IDENTIFICADOR ÚNICO	FUNCIONES	CATEGORÍA IDENTIFICADOR ÚNICO	CATEGORIAS
ID	IDENTIFICAR	ID.AM	Gestión de activos
		ID.BE	Ambiente de negocios
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	PROTEGER	PR.AC	Gestión de identidad, autenticación y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología de protección
DE	DETECTAR	DE.AE	Anomalías y Eventos
		DE.CM	Monitoreo continuo de seguridad
		DE.DP	Procesos de Detección
RS	RESPONDER	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
		RS.RP	Planificación de respuesta
RC	RECUPERAR	RC.RP	Planificación de la recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Niveles de implementación

NIVEL	TIPO	PROCESO DE GESTIÓN DE RIESGOS	PROGRAMA DE GESTIÓN INTEGRADA DE RIESGOS	PARTICIPACIÓN EXTERNA
1	PARCIAL	No se formalizan las prácticas organizativas de gestión de riesgos de ciberseguridad y se gestiona el riesgo de manera ad hoc ya veces reactiva.	Se conoce muy poco el riesgo de ciberseguridad a nivel organizativo y no se ha establecido un enfoque de gestión del riesgo de ciberseguridad en toda la organización.	Puede no tener los procesos establecidos para participar en la coordinación o colaboración con otras entidades.
2	RIESGO INFORMADO	Las prácticas de gestión de riesgos son aprobadas por la administración pero no pueden establecerse como políticas de toda la organización.	Se conoce el riesgo de ciberseguridad a nivel organizativo, pero no se ha establecido un enfoque a nivel de toda la organización	La organización conoce su papel en el ecosistema más grande, pero no ha formalizado sus capacidades para interactuar y compartir información externamente.
3	REPETIBLE	Las prácticas de gestión de riesgos de la organización son formalmente aprobadas y expresadas como políticas.	Existe un enfoque a nivel de toda la organización para gestionar el riesgo de la ciberseguridad.	La organización entiende sus dependencias y socios y recibe información que permite la colaboración y las decisiones de gestión basadas en el riesgo
5	ADAPTATIVO	La organización adapta sus prácticas de ciberseguridad basadas en las lecciones aprendidas y los indicadores predictivos	Existe un enfoque a nivel de toda la organización para gestionar el riesgo de ciberseguridad que utiliza políticas, procesos y procedimientos	la organización gestiona el riesgo y comparte activamente la información con los socios para garantizar que se distribuye información precisa para mejorar la ciberseguridad antes de que se produzca un evento

Los tiers proporcionan un contexto sobre cómo una organización ve el riesgo de la ciberseguridad y los procesos implementados para manejarlo. Las escalas describen el grado en que las prácticas de gestión de riesgos cibernéticos de una empresa exhiben las características definidas en el marco. Por ejemplo: riesgo y amenaza, repetible y adaptable.

Los niveles de implementación caracterizan las prácticas de una compañía en un rango, desde parcial hasta adaptativo. Estos niveles reflejan una progresión desde respuestas informales y reactivas hasta enfoques que son ágiles y están informados sobre el riesgo. Durante el proceso de selección de un tier, la empresa debe considerar sus actuales prácticas de gestión de riesgos, entorno de amenazas, requisitos legales y regulatorios, objetivos de negocio/misión y restricciones de organización.

Gestión de incidentes de ciberseguridad

¿Qué es la gestion de incidentes?

De acuerdo a lo que se indica en las funciones del núcleo de ciberseguridad ya revisadas, la gestión de incidentes comprende la asignación de roles y responsabilidades para el desarrollo de actividades ante la ocurrencia de incidentes.

Una de las funciones del Responsable de Seguridad de la Información / Ciberseguridad es la coordinación de acciones conjuntas con las partes interesadas para atención de incidentes.

El proceso de gestión de incidentes debe estar enmarcado en la mejora continua, que permita mejorar actividades para futuros incidentes. Los resultados de la gestión de incidentes deben ser documentados; esto permitirá analizar y realizar mejoras a controles existentes o implementar nuevos.

Etapas de la gestión de incidentes

Gestión del cumplimiento

¿Qué es la gestión del cumplimiento?

El cumplimiento o “compliance” en inglés es, netamente, el cumplimiento normativo que debe tener la Organización en términos de cumplimiento normativo. u ámbito de aplicación está relacionado con las buenas practicas dentro de las organizaciones. En algunas ocasiones estas adoptan un conjunto de procedimientos y buenas prácticas cuyo objetivo es identificar y clasificar los riesgos operativos y legales a los que se enfrentan. Así se podrán establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos.

¿Qué es la gestión del cumplimiento?

Por qué es necesario contar con un Sistema de Gestión de cumplimiento legal?

Contar con un Sistema de Gestión Compliance, puede beneficiar a las organizaciones en cuatro aspectos fundamentales:

- En relación con los intereses comerciales: aumentará la reputación de la organización, así como su imagen de marca. En el caso de las empresas, mejorará la percepción de la empresa y sus productos de cara a clientes y proveedores, favoreciendo así el incremento de la actividad comercial. Por otro lado, contribuirá a cumplir las condiciones que las grandes empresas solicitan a sus proveedores, etc.
- Desde el punto de vista económico: ayudará a detectar el uso indebido de medios propios de la compañía, así como hurtos, robos, y actitudes impropias de directivos, mandos intermedios, empleados y proveedores. Todos esto minimizará gastos.
- Con respecto al funcionamiento de la organización: va a contribuir a mejorar el clima de la organización, así como el comportamiento de todos los trabajadores. Además, contribuirá a mejorar la comunicación y la confianza en el seno de la empresa.
- A nivel jurídico, también puede aportar muchas ventajas: acreditando que existe un sistema de control adecuado a las exigencias de la ley y se cumple con la normativa vigente a nivel de compliance. Por otro lado, ayudará a eximir a la propia compañía de responsabilidad penal, evitando la imputación de la empresa en el caso de que se cometa un delito en su entorno, protegiéndola sobre todo de posibles multas.

Gestión de la continuidad de negocio

¿Qué es la gestión de la continuidad del negocio?

La Gestión de la Continuidad del negocio es el proceso de lograr esta capacidad y mantenerla, y conforma una parte vital de la gestión de seguridad de sistemas de información, que ahora se conoce más comúnmente como seguridad cibernética.

Etapas de la gestión de la continuidad del negocio

Identificar y ordenar las amenazas

Realizar un análisis de impacto a la Organización

Crear un plan de respuesta y recuperación

PROBAR EL PLAN Y REFINAR EL ANÁLISIS!

Gestión de la cultura en Ciberseguridad

¿Qué es la gestión de la cultura en Ciberseguridad?

Igual que realizamos controles médicos de empresa y concienciamos en materia de prevención de riesgos laborales a nuestros empleados, también es importante concienciarles y formarles en materia de ciberseguridad.

Esta formación en ciberseguridad creará una cultura de seguridad en la empresa que servirá para establecer las bases de la protección, tanto de nuestra información confidencial, como la de nuestros clientes y proveedores.

Debemos fomentar el desarrollo de esta cultura de seguridad formando a nuestros empleados en ciberseguridad, teniendo siempre presente las políticas, normativas y procedimientos de seguridad establecidas en la empresa; supervisando que se cumplen las buenas prácticas en seguridad establecidas; y realizando acciones de sensibilización y concienciación en seguridad para empleados de manera continua.

¿Cómo manejamos la cultura en Ciberseguridad?

Usuaria ingresa a la organización

Una vez dentro, se le explican las Normativas de la organización, NDA, etc., las cuales deberá aceptar

Usuaria será capacitada por la organización en su Cultura, y como se abordan las normativas

Usuaria tendrá acceso a la información, y ya sabe como actuar ante ciertos eventos.

De repente, la Organización se ve atacada por un evento malicioso

La organización contacta a los encargados y logran sobrellevar el evento

La información y accesos se ha visto afectados por este evento.

Se realizan comités y se revisa la información del evento

Se actualiza la documentación asociada, y se generan lecciones aprendidas

Se vuelve a capacitar al equipo y se distribuye la documentación actualizada

Se realizan campañas de concientización constantemente

¿Qué podemos aprender?

- En muchas ocasiones, la brecha de seguridad se ve impactada por los mismos usuarios, ya que ellos no reciben las capacitaciones ni la información de accesos de la Cultura de Ciberseguridad y Seguridad de la Información, más que por la propia brecha tecnología. **Nuestros usuarios son primero.**
- El comité de seguridad debe estar compuesto por un representante de cada área de la organización, esto indica la necesidad de contar con áreas de Negocio, ya que es importante que ellos también sean partícipes de la Seguridad de la organización, además de Gerentes, que aportarán en la Cultura de Ciberseguridad y Seguridad de la Información.
- La documentación, revisada en comité, puede sufrir cambios del tipo Legislativo, Organizativo, tecnológico (considerar que esto es bajo un escenario normal, ya que frente a eventos de Seguridad, normalmente éstos serán actualizados).
- Siempre mantener los canales de difusión y comunicación actualizados y de fácil acceso para todos los integrantes de la Organización, claro, entendiendo que a veces podrían estar segmentados según el tipo de información a la que pueden tener acceso.

Lecciones aprendidas

Siempre gestionar riesgos

Siempre estar alerta ante posibles riesgos de ciberseguridad y de seguridad de la información, actualizar y analizar.

Mantener una mejora continua en la gestion de incidentes

Siempre aprender de cada incidente ocurrido y poner en práctica lo aprendido y documentar, para así mantener una mejora continua en el ciclo de un incidente

Siempre actualizar ciberescenarios para mantener la continuidad del negocio

Siempre considerar escenarios de amenazas y vulnerabilidades cibernéticas en nuestros DRP y ¡probarlos siempre!

Concientizar y evangelizar

Los trabajadores de la Organización deben ser y estar conscientes de los riesgos de ciberseguridad a los cuales estamos expuestos.

12 MARZO 2021

II CONGRESO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

¡Muchas Gracias!

Gobierno y Gestión de la Ciberseguridad

Speakers:

Mg. Bárbara Palacios Cabezas
Ing. Constanza Herrera Pizzoleo

Linkedin

https://cl.linkedin.com/in/bpalaciosc
https://www.linkedin.com/in/ConstanzaHerreraPizzoleo

SOCHISI
DIGITAL SECURITY THINK TANK

HACKADA

SOCHISI.CL/ENVIVO