2022

Governance | Risk | Compliance | Audit

SUMMIT GIT 2022

AUDITANDO LA CIBERSEGURIDAD.

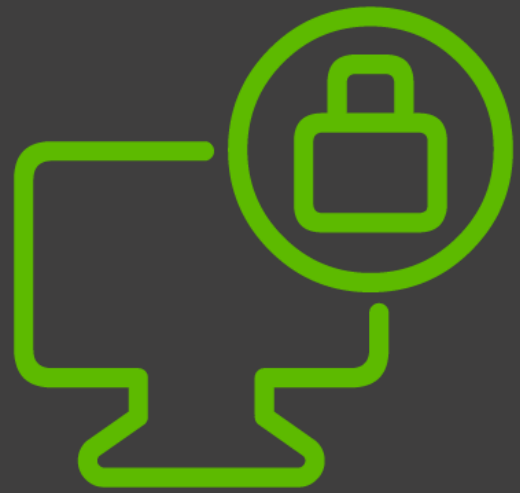
¿USANDO EL MARCO DE CIBERSEGURIDAD DEL NIST? ¿CON LOS CONTROLES CIS®? ¿AMBOS?


Server has crashed
Where is backup?
On the server

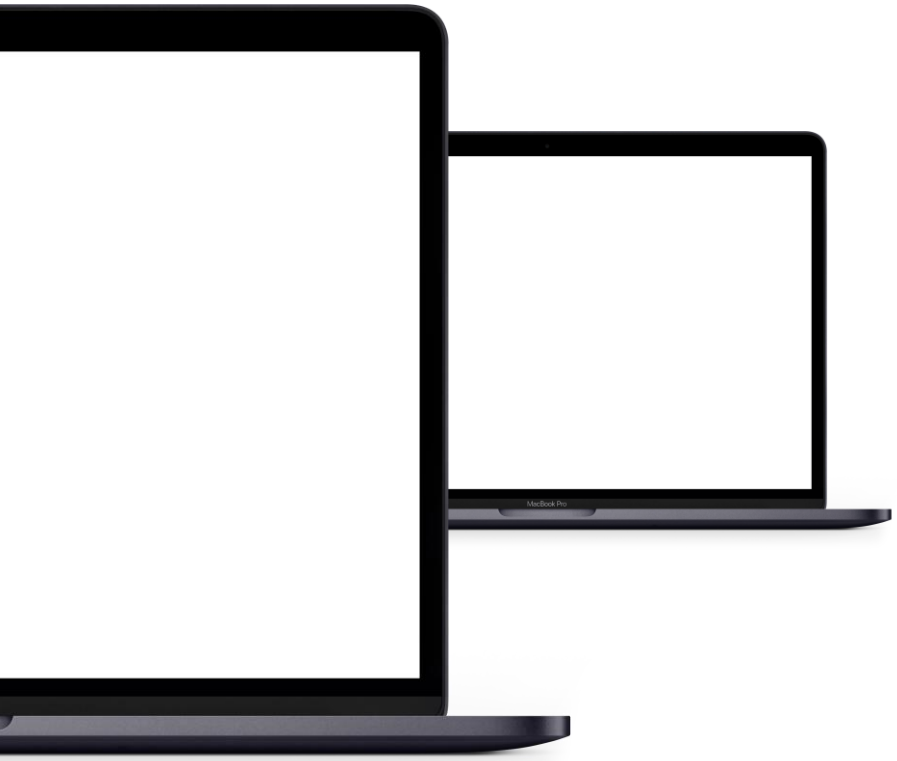

IT SECURITY:
YOU PASSED THE
PHISHING TEST
ME WHO
NEVER OPENS
ANY EMAILS

UNA CORTA INTRODUCCIÓN

¿En qué piensan cuando escuchan la palabra CIBERSEGURIDAD?



CIBERSEGURIDAD



La protección de los **activos digitales**, abordando las amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados.

La triada de la ciberseguridad

Protección de la información contra el acceso no autorizado o la divulgación indebida de acuerdo con su sensibilidad y los requisitos legales aplicables.

La información debe ser accesible cuando se requiera

Protección de la información contra la modificación no autorizada. La información se debe mantener inalterada ante accidentes o intentos maliciosos

Cámara Colombiana de Informática y Telecomunicaciones

Fuente: CIBER-SEGURIDAD EN LA ERA DE LA MOVILIDAD DIGITAL

Principales amenazas

Algunas cifras…

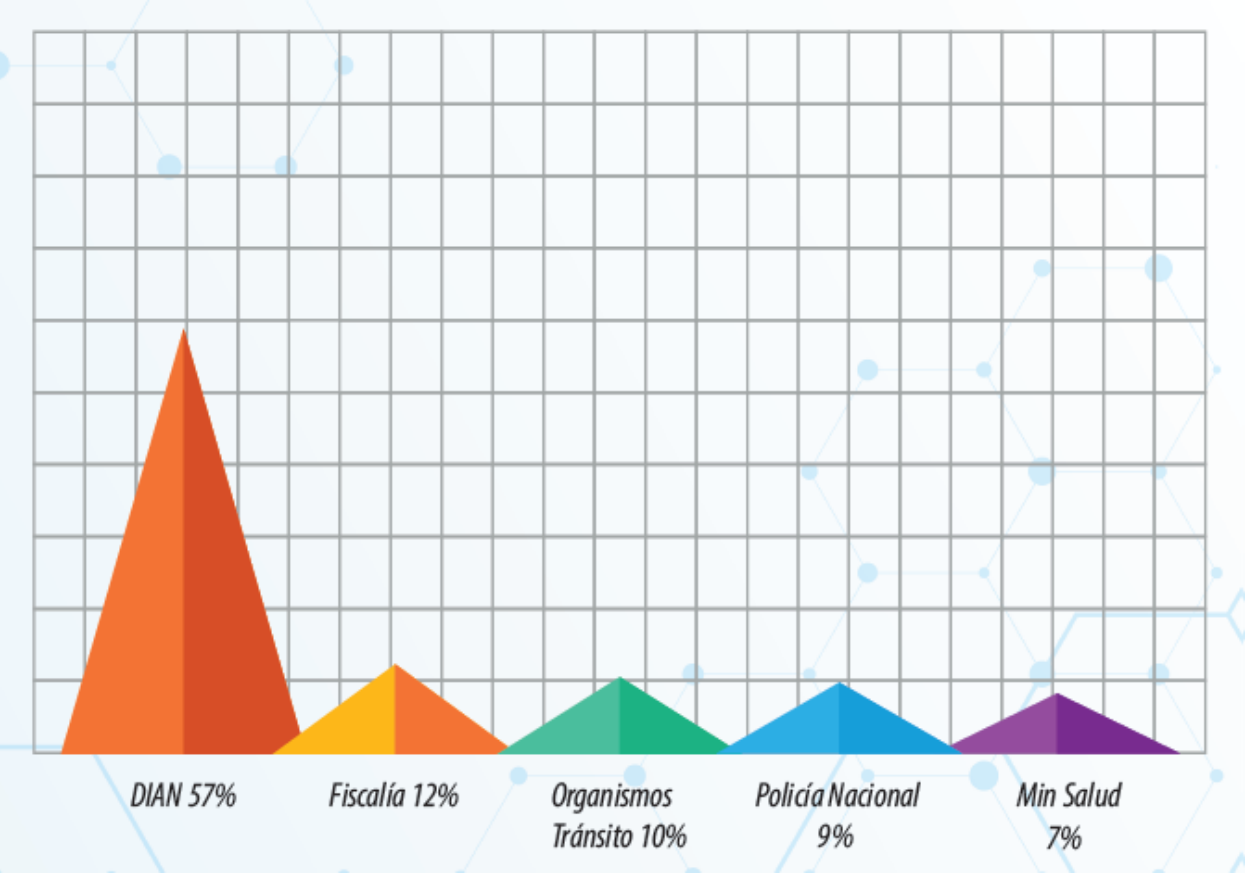
Delitos con mayor crecimiento durante el 2021:

- La Violación de Datos Personales con 13.458 casos, es el delito de mayor crecimiento en el país durante el 2021.
  - ✓ Ataques de Phishing.
  - ✓ Principalmente datos bancarios, nombres y apellidos de la víctima, documento de identidad, lugar de nacimiento y demás información necesaria para adelantar trámites y generar procesos fraudulentos.
- La segunda modalidad de mayor crecimiento es el acceso abusivo a sistemas informáticos: 9.926 denuncias, y un incremento del 18% respecto 2020.
  - ✓ Fases iniciales de un ciberataque, para luego escalar privilegios.
- En tercer lugar, se encuentra el hurto por medios informáticos. Se han instaurado 17.608 denuncias desde enero hasta noviembre del 2021.
- La suplantación de sitios web con 7.654 casos tuvo un incremento similar del 3% respecto al año 2020, siendo el Phishing y el Smishing las principales modalidades empleadas por los Cibercriminales.

Fuente: Tendencias del cibercrimen 2020-2021

Principales amenazas

Algunas cifras…



Asuntos más utilizados en las campañas de phishing:

- Notificación de comparendos.
- CC reportada como robada
- Notificación de órdenes de embargo.
- Notificación de citación a audiencias.

Principales amenazas

- El malware en evolución, nuevas técnicas para evadir los Antivirus.
- Principal método de infección: descargas de apps en tiendas y mercados no autorizados.
- El Smishing como vector de ataque seguirá creciendo. SMS o mensajes por aplicaciones de mensajería con un enlace a una aplicación con malware.
- Los programas maliciosos obtienen control total sobre el dispositivo.
- Acceso remoto por parte del atacante.
- Se observan también fuentes como archivos de Word, Excel o PDF.

Cámara Colombiana de Informática y Telecomunicaciones

Fuente: CIBER-SEGURIDAD EN LA ERA DE LA MOVILIDAD DIGITAL

AUDITANDO LA CIBERSEGURIDAD

Preguntas clave

Para iniciar con la auditoría, debemos validar dos aspectos clave:

1 ¿La compañía ha identificado y clasificado los Activos de Información?

2 ¿Se han identificado y gestionado los riesgos a los que están expuestos estos activos de información?

Gestión de los Activos de Información

1

Inventario de Activos
Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos de información de la organización.

2

Propiedad y custodia de los Activos
Todos los activos deben ser propiedad de una parte designada y custodiados.

3

Directrices de Clasificación de Activos
La información debe clasificarse en términos de su valor, de los requisitos legales, de su sensibilidad y la importancia para la organización.

4

Tratamiento de Activos
Se debe establecer qué controles mínimos deben ser aplicados a los activos, dependiendo su nivel de clasificación.

Gestión de los Activos de Información

Las compañías deben levantar un inventario de los activos de información, donde estos se puedan clasificar según su criticidad y confidencialidad.

Tipo de Activo
Información, software, hardware, servicios, infraestructura, recurso humano y auxiliares.

Información General
Nombre, descripción, proceso al que pertenece, información complementaria.

Propiedad
Quién es el propietario y quién es el custodio.

Clasificación del Activo
Reservada, Confidencial, Privada, Interna y Pública

Confidencialidad, Disponibilidad, Integridad y Privacidad
Crítico, Alto, Medio, Bajo y Muy bajo

Riesgos sobre los activos

GESTIÓN DE RIESGOS

Los riesgos sobre los activos deben estar identificados y evaluados.

MATRIZ DE RIESGOS

Los riesgos deben estar actualizados y monitoreados.

¿Y SI NO SE TIENE CONFIANZA?

El auditor debe hacer el proceso de la identificación y valoración de riesgos, según su expertis y conocimiento de la compañía.

¿Qué evaluar del inventario y riesgos de los activos?

1. ¿Se cuenta con un inventario actualizado?
2. ¿Están clasificados y valorados los activos? ¿Hay escalas definidas?
3. ¿Se tienen en cuenta requerimientos normativos, contractuales y demás?
4. ¿La matriz de riesgos está actualizada?
5. ¿Se evalúan riesgos sobre los activos más relevantes?
6. ¿Se define la respuesta según la evaluación de riesgos?

¿Qué evaluar del inventario y riesgos de los activos?

Niveles de riesgo	Respuesta
BAJO	ACEPTAR
MEDIO	ACEPTAR – MITIGAR - TRANSFERIR
ALTO	MITIGAR – TRANSFERIR
MUY ALTO	MITIGAR - TRANSFERIR

¿NIST O CIS CONTORLS?

The Cybersecurity Framework - NIST

El Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology), llamada entre 1901 y 1988 Oficina Nacional de Normas (NBS por sus siglas del inglés National Bureau of Standards), es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica.

https://www.nist.gov/cyberframework/framework

The Cybersecurity Framework - NIST

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

5 Functions 23 Categories 108 Subcategories 6 Informative References

https://www.nist.gov/cyberframework/framework

CIS Controls

El framework del CIS desglosa 18 grupos de control de seguridad de la información y los organiza en 3 categorías:

IG1
Grupo de implementación 1

IG2
Grupo de implementación 2

IG3
Grupo de implementación 3

https://www.cisecurity.org/controls/cis-controls-navigator/

CIS Controls

https://www.cisecurity.org/controls/cis-controls-navigator/

CIS Controls

IG1

Una empresa IG1 es de tamaño pequeña a mediana con experiencia limitada en TI y ciberseguridad para dedicarse a proteger los activos y personal de TI. La principal preocupación de estas empresas es mantener el negocio operativo, ya que tienen una tolerancia limitada de inactividad. La sensibilidad de la información que ellas tratan de proteger es baja y principalmente incluye información de empleados e información financiera.

Las Salvaguardas seleccionadas para IG1 deberían ser implementables con limitada experiencia en ciberseguridad y estar dirigidas a frustrar ataques generales y no dirigidos. Estas Salvaguardas normalmente se diseñan para trabajar en conjunto con software y hardware que ya existe y se encuentra disponible de fuentes comerciales (COTS).

https://www.cisecurity.org/controls/cis-controls-navigator/

CIS Controls

IG2 (Incluye IG1)

Una empresa IG2 emplea a individuos responsables de administrar y proteger la infraestructura de TI. Estas empresas se apoyan de múltiples departamentos con distintos perfiles de riesgo en base a la función del puesto y misión. Las empresas IG2 almacenan procesos e información sensible sobre el cliente o información empresarial y pueden soportar breves interrupciones de servicios. La mayor preocupación es la pérdida de la confianza del público si se produce una brecha.

Las Salvaguardas seleccionadas para IG2 ayudan a los equipos de seguridad a hacer frente al incremento de la complejidad operacional. Algunas Salvaguardas están sujetas al grado de tecnología y nivel empresarial, experiencia especializada para ser instaladas y configuradas correctamente.

https://www.cisecurity.org/controls/cis-controls-navigator/

CIS Controls

IG3 (Incluye IG1 y IG2)

Una empresa IG3 emplea expertos en seguridad los cuales se especializan en diferentes facetas de la ciberseguridad (por ejemplo, gestión de riesgo, pruebas de penetración, seguridad en las aplicaciones). Los activos e información IG3 contienen información sensible o funciones que están sujetas a supervisión regulatoria y de cumplimiento. Una empresa IG3 debe abordar la disponibilidad y la confidencialidad e integridad de los datos sensibles. La materialización de los ataques puede causar un daño significativo al bienestar público.

Las Salvaguardas seleccionadas para IG3 deben reducir los ataques dirigidos por un adversario sofisticado y reducir el impacto de los ataques de día cero.

https://www.cisecurity.org/controls/cis-controls-navigator/

CONCLUSIONES

Conclusiones

- Lo que no está identificado e inventariado, no se puede proteger.
- Revisar la matriz de riesgos sobre los activos, si no se confía, identificar y valorar los propios.
- Todos los activos representan un valor distinto para la organización y por lo tanto, se deben proteger de maneas distintas.
- Soportarse en marcos metodológicos nos facilita el trabajo.
- Se debe aterrizar el marco metodológico a la operación de la organización.

¡¡¡MUCHAS GRACIAS!!!

Abit CONSULTORÍA

FERNEY ANDRÉS ALVARADO OSPINA

Ingeniero de Sistemas de la Universidad Icesi. Auditor y Consultor de TI. Certificado CISA, COBIT 2019, Advanced SOC for Service Organizations y Scrum Foundations. Instructor acreditado CISA por APMG. Más de quince años de experiencia en diferentes firmas de auditoría (top ten worldwide) como Auditor y Consultor de Informática. Presidente de **ISACA Medellín Chapter**. Fundador y Director General de **ABIT CO**

Ponente en diferentes eventos de tecnología nacionales y regionales, docente de la especialización de ciberseguridad de la Universidad Autónoma de Occidente, instructor de cursos impartidos por ISACA Medellín, la Cámara de Comercio de Cali y la Cámara de Comercio de Medellín para Antioquia.

linkedin.com/in/ferneyalvarado/

+57 300 452 33 38

ferney@abit-co.com

www.abit-co.com