Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

Transmisión a través de:

Blackboard

Escuchemos a:

Maria Angelica Castillo
Experta en tecnologias digitales, interoperatibilidad ciberseguridad e IA aplicada

Mayor Marlon Mike Toro
Director Centro de Innovación y Ciencia de Policía POLIS
Policia Nacional de Colombia

Nazly Borrero
Directora Colombia Cibersegura

Gustavo Guzmán
Académico y especialista en Gobierno de TI y Ciberseguridad

Phd. Carlos Castañeda
Investigador Ciberseguridad y Ciberdefensa
Escuela Superior de Guerra

David Pereira
CEO Secpro

Juan David Cardona
Director Estratégico de la Compañia Arcont Group SAS

Coronel (RP) Fredy Bautista
Consultor Programa SAFE CCIT | Director Centro Cibernético Policial en años 2002- 2018

Andres Ricardo Almanza Junco
CGO CISOS Club

Ana Maria Mesa
CEO en Law Tic Grupo Jurídico

Moderador | Aristides Contreras
Presidente Comunidad COLADCA y Líder ExcyberProject Excelencia en Ciberseguridad

Emanuel Ortiz
Director de la Red Ciber y la Asociación ASIIF

Felix Augusto Reyes
Autor del Libro Amenazas informáticas en la Web 3.0

Sandy Palma
Presidente Honduras Cibersegura

ESCUELA DE POSTGRADOS
FUERZA AÉREA COLOMBIANA
VIGILADA MINEDUCACIÓN

MAESTRÍA EN
DIRECCIÓN Y GESTIÓN DE LA SEGURIDAD INTEGRAL
ESCUELA DE POSTGRADOS FAC / SNIES 105360

Conectate vía:

Fecha: 18 de Marzo de 2020
Hora: 17:00 Hrs a 19:00 Hrs
(UTC-05:00) Bogotá, Lima, Quito

Cupo y Preregistro:
https://bit.ly/2IX7C3o

Organizan y apoyan

Presentación

Memorias Webinar sobre Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

Entre los pasados 12 y 29 de diciembre de 2019, "según las autoridades de salud de Wuhan en China" se detectaron unos primeros casos de neumonía y fueron reportados a la Organización Mundial de la Salud; durante este periodo, el virus (COVID-19) aún desconocido, no mostraba la cara de su poder ni lo que vendría para nuestro mundo.

A la fecha de escribir estas lineas y culminando la compilación de las memorias que dejamos a su disposición, veo que **más del 80% de la población mundial vive una gran incertidumbre, decretos de cuarentena, aislamiento obligatorio y noticias de muertos cada día.** Las empresas y diferentes organizaciones buscan oportunidades para la continuidad de sus operaciones y negocios; hoy la mayoría de los seres humanos, aún sin ser lastimados como ha sido para Europa y en especial para Italia con más de 1000 muertos, hemos sido enviados a nuestras casas y desde allí a realizar actividades usando la Internet.

Sin importar la critica situación que vive el mundo, **la Criminalidad digital se ha disparado usando diferentes métodos para aprovechar las circunstancias, la falta de información, las confusiones y todo lo que gira en torno a la Pandemia por Coronavirus**, aun así debemos seguir conectados a nuestra Laptop, tablet o celular, para enviar y recibir correos electrónicos, ingresar al banco, pagar servicios y por supuesto, revisar nuestras redes sociales.

Surgen inmediatamente grandes retos que fueron debatidos con expertos en la materia y que a continuación darán sus recomendaciones.

A continuación encuentran:

1. Consejos y recomendaciones de Seguridad Digital por parte de **Maria Angelica Castillo desde Lima - Perú.**
2. Detalles a tener cuenta para una conexión segura por parte de **Gustavo Guzmán de Ciudad de México.**
3. Buenas practicas aplicada al uso de la tecnología por **Nazly Borrero desde Cali - Colombia.**
4. Preocupaciones por alerta Global de Ciberataques y otros delitos usando la pandemia como escudo por el **Coronel (RP) Fredy Bautista García, desde Bogotá – Colombia.**
5. Importantes recomendaciones para administradores de TI y Aseguramiento digital de estaciones de trabajo por **David Pereira, desde Bogotá – Colombia.**
6. El Decálogo de Humanidad y Seguridad para trabajar en el mundo digital a través del Teletrabajo por **Andres Ricardo Almanza, desde Bogotá – Colombia.**
7. La Guia de Supervivencia ante Ingeniería Social por **Emanuel Ortiz, desde Bogotá – Colombia.**
8. Los Riesgos laborales del teletrabajo, viéndola desde una perspectiva mixta, vinculando las TIC´s al Derecho por **Juan David Cardona, desde Leon - España**
9. El Nivel de madurez para contingencia en la pequeña y gran empresa por **Carlos Castañeda PhD. Desde Bogotá – Colombia.**
10. Los Riesgos técnico-legales que afectan la seguridad de la empresa con el acceso a sus aplicativos, desde dispositivos personales en empleados y contratistas, por **Ana Maria Mesa PhD. Desde Medellín - Colombia.**
11. Recomendaciones de Seguridad Digital para cumplir planes preventivos de protección de Datos por **Sandy Palma desde Tegucigalpa - Honduras.**

A tod@s, nuestro mayor agradecimiento por su tiempo y por vincularse en el propósito para seguir **"Dejando Huella"** desde **COLADCA** en materia de **prevención de Riesgos digitales** para ustedes! **Los lectores.**

Temáticas propuestas

18 Marzo
17:00 a 19:00

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

Planes preventivos
de proteccion de Datos

Consejos y Recomendaciones
de seguridad digital para las
compañías en el Teletrabajo

Conexiones Seguras
¿Y los Adminitradores de Red?

Como evitar que estrategias BYOD
se conviertan en una amenaza interna
extendida en escenarios de Teletrabajo

Decalogo de Seguridad para el Teletrabajo
Con diciones humanas y de Seguridad Digital

Riesgos Tecnico Legales que afectan
Seguridad de la Empresa
Acceso aplicativos de Empleados y Contratistas

Vulnerabilidades al modo de pensar
del teletrabajador.
vectores de ataque e ingenieria social.

Buenas practicas y concientizacion
efectiva de empleados y colaboradores
en trabajo remoto.

Controles
Recomendaciones para
las areas de TI

VPN – Nube – Aseguramiento
digital de estaciones de trabajo
De dispositivos a redes locales
de Empresa

ABC de los Peligros y Amenazas
informaticas. a que se expone al navegar
en la Internet

Introducción

Dr. Aristides Contreras Fernández

Presidente Comunidad COLADCA

Líder Excyber Project | Proyecto de Excelencia en Ciberseguridad

Aliados COLADCA

INTRODUCCIÓN

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

Seguridad Digital y Ciberseguridad En Teletrabajo

| An Unsettled World |
Un mundo inestable
WEF

Aristides Contreras
Moderador
Presidente COLADCA
www.coladca.com
@Aris_Contreras_

18 Marzo | 2020

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

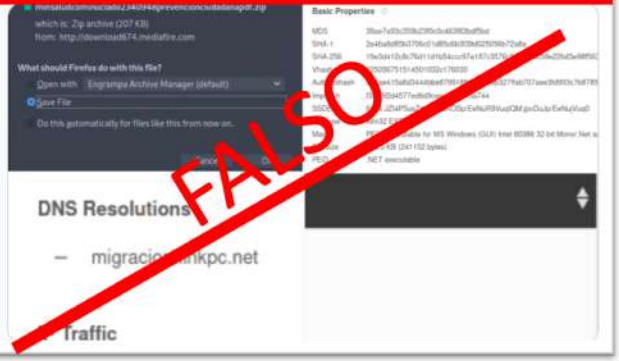
CONTEXTO

CCN-CERT @CCNCERT

Los cibercriminales están aprovechando la pandemia de #coronavirus para realizar múltiples campañas de malware, incluyendo #ransomware. Creamos este hilo para ir notificando las más importantes. ¡Síguenos! #NoTeinfectesConElMail. #CiberCOVID19

colCERT @colCERT · 6 mar.

¡Alerta! IoCs sobre el correo electrónico malicioso con asunto "Detectamos en su sector la presencia de COVID-19 (Corona virus) intentamos comunicarnos via telefonica con usted" que está circulando a nombre de @MinSaludCol #phishing #malware @Ministerio_TIC @CaiVirtual



Ataques de #malware utilizando el troyano #Netwire mediante un engaño por e-mail para obtener consejos procedentes de @UNICEF frente al #Coronavirus. ¡No caigas!

From UNICEF Inc <swift@allcounty.com>
Subject UNICEF COVID-19 TIPS APP
To Recipients <swift@allcounty.com>

Find attached presentation & APP regarding COVID-19 for your reference and dissemination. kindly download and install on your system for dearly update and guide line on how to protect your self and staff from this current deadly virus

Kindly pass it on, Let join hand together and fight this virus to the last.

Thanks
1-760-597-2966 ext 135

unicef

FALSO

CONTEXTO

@ThreatCloud descubre una campaña contra el sector público de Mongolia. #NoTeInfectesConElMail #CiberCOVID19

Vicious Panda: The COVID Campaign - Check Point Research
Introduction Check Point Research discovered a new campaign against the Mongolian public sector, which takes advantage of the current Coronavirus ...
research.checkpoint.com

RIESGOS

"DE NATURALEZA COMPLEJA Y MULTIVECTORIAL"

WEBINAR

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

RIESGOS

1

2

3

En el número de ataques cibernéticos, la tendencia es obvia, están aumentando

Mirek Dusek | Presidente del Foro Económico Mundial,

Figure I: The Evolving Risks Landscape, 2007–2020

Top 5 Global Risks in Terms of Likelihood

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
st	Infrastructure breakdown	Blow up in asset prices	Asset price collapse	Asset price collapse	Storms and cyclones	Income disparity	Income disparity	Income disparity	Interstate conflict	Involuntary migration	Extreme weather	Extreme weather	Extreme weather	Extreme weather
nd	Chronic diseases	Middle East instability	China economic slowdown	China economic slowdown	Flooding	Fiscal imbalances	Fiscal imbalances	Extreme weather	Extreme weather	Extreme weather	Involuntary migration	Natural disasters	Climate action failure	Climate action failure
rd	Oil price shock	Failed and failing states	Chronic diseases	Chronic disease	Corruption	Greenhouse gas emissions	Greenhouse gas emissions	Unemployment	Failure of national governance	Climate action failure	Natural disasters	Cyberattacks	Natural disasters	Natural disasters
th	China hard landing	Oil price shock	Global governance gaps	Fiscal crises	Biodiversity loss	Cyberattacks	Water crises	Climate action failure	State collapse or crisis	Interstate conflict	Terrorist attacks	Data fraud or theft	Data fraud or theft	Biodiversity loss
th	Blow up in asset prices	Chronic diseases	Deglobalization (emerging)	Global governance gaps	Climate change	Water crises	Population ageing	Cyberattacks	Unemployment	Natural catastrophes	Data fraud or theft	Climate action failure	Cyberattacks	Human-made environmental disasters

POR PRIMERA VEZ THE GLOBAL RISK REPORT 2020

IDENTIFICA RIESGOS MEDIOAMBIENTALES

"Como las amenazas globales más probables"

CIBERATAQUES

WORLD ECONOMIC FORUM

WEBINAR

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

Generar participación y concientización en todas las areas de la organización, en materia de Gestión de Riesgos es Fundamental y Necesario.
"LOS PROPIETARIOS DEL RIESGO SOMOS TODOS"

Valorar lo aprendido

Reaprender

Metas y Recomendaciones

COLADCA

EX CYBER PROJECT

CISO's

Conferencia 1 de 11

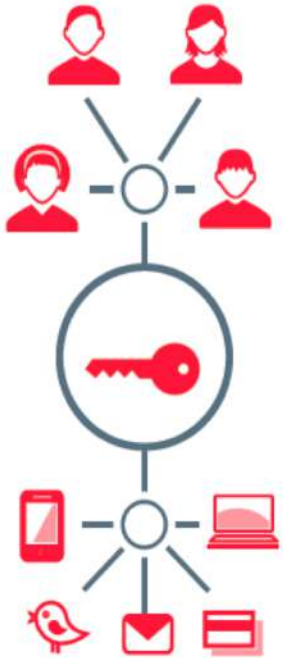
MSc. Maria Angelica Castillo

Experta en tecnologías digitales, interoperatibilidad
Ciberseguridad e IA aplicada
Parte de HackLab Girls Latam
Líder y parte del Comité de Expertos COLADCA
Capítulo Perú

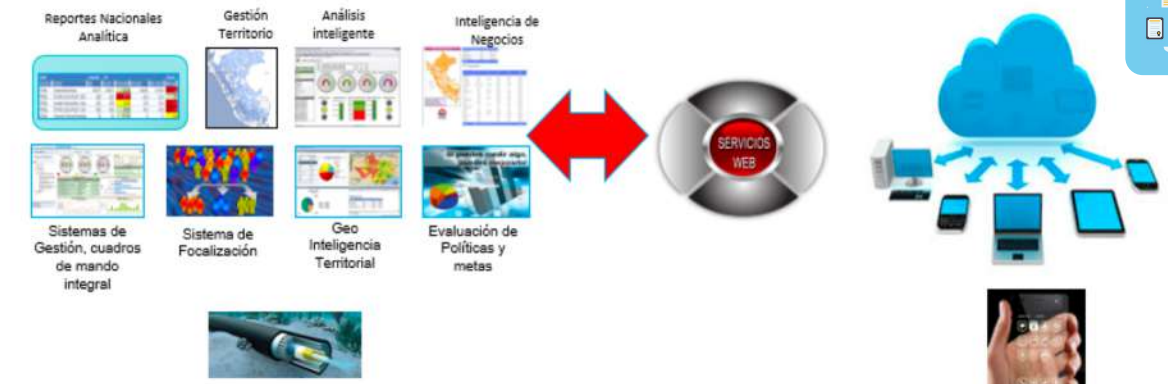
CONFERENCIA 1 DE 11

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

Consejos y Recomendaciones de seguridad digital para las compañías en el Teletrabajo

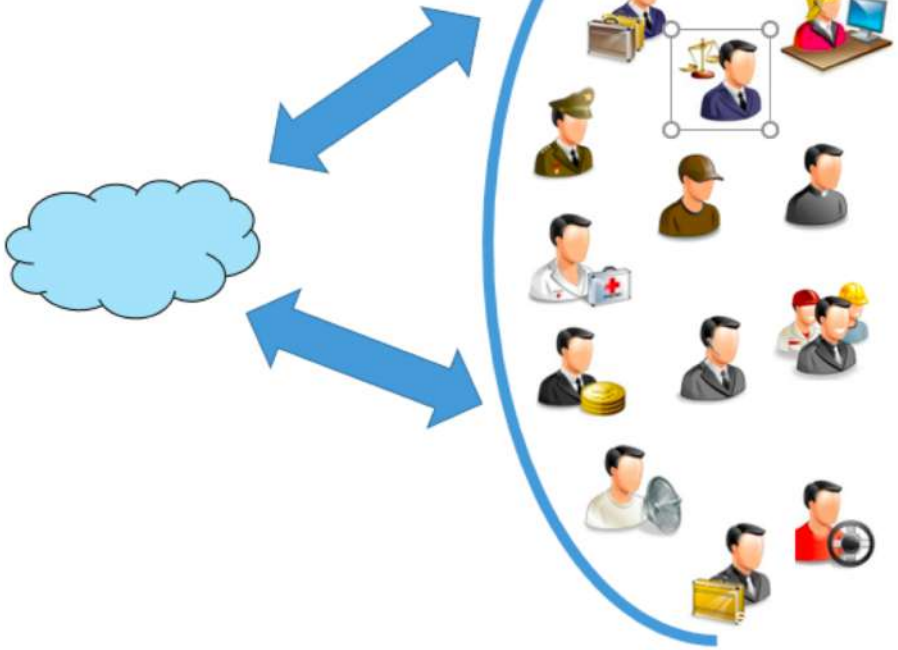


MSc. Ing. M. Angélica Castillo Ríos



BASES DE DATOS

INTEROPERABILIDAD



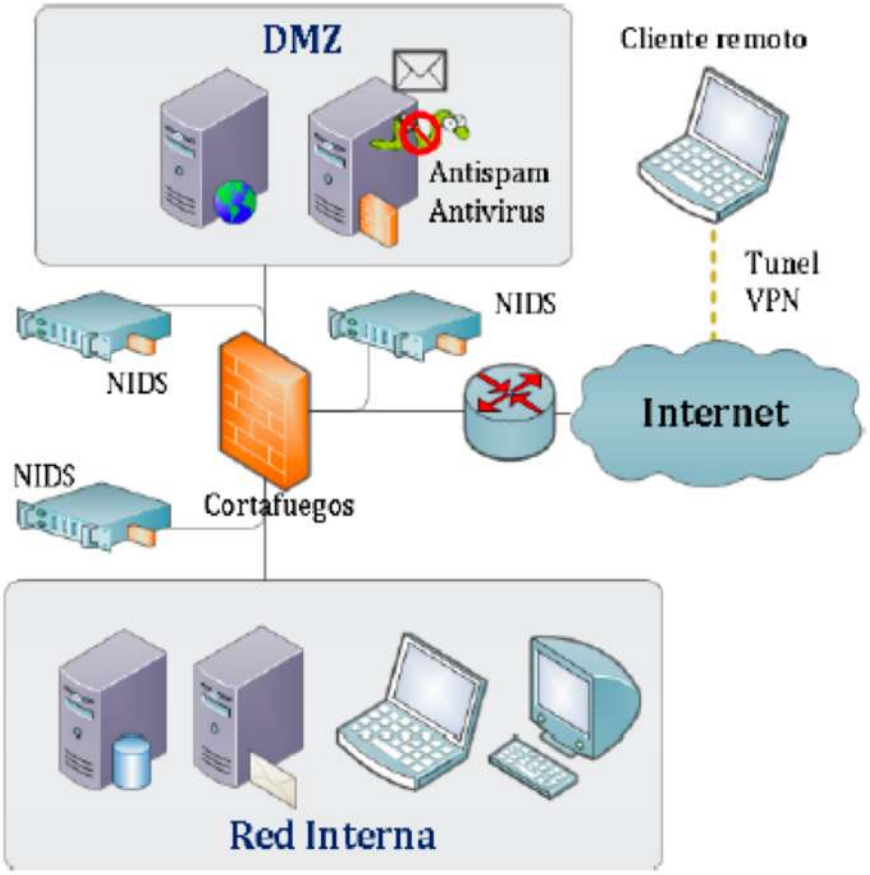
Elementos que proveen seguridad al perímetro

1. Antivirus, antispam
2. Firewall o Corta fuego
3. Redes virtuales privadas (VPN)
4. DMZ o Zona desmilitarizada
5. Sistema de detección y prevención de Intrusos (IDS/IDPS)
6. Anti DDOS (Distributed Denial of Service), ataque de denegación de servicio distribuido

Arquitectura con seguridad perimetral

- ✓Instalación de antispam y antivirus.
- ✓Instalación de Firewall
- ✓Clientes remotos usan VPN.
- ✓DMZ y Red Interna
- ✓Instalación de IDPS en las tres interfaces.

- ✓Wi-Fi Seguro
- ✓HTTPS: comunicaciones cifradas a través de SSL/TSL
- ✓Autenticación multi-factor y tokens de seguridad
- ✓Seguridad de la navegación web
- ✓Encriptación de voz y data
- ✓Hackeo Etico
- ✓Switch gestionados
- ✓Análisis de vulnerabilidad en código fuente
- ✓WAF (Web Application Firewall) protege servidores de aplicaciones web, evita ataques:



Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

HackLabGirls Latam

TELETRABAJO ¿SEGURO?

Ciberconsejos para #quedarteEnCasa

UTILIZA DISPOSITIVOS PROVISTOS POR LA EMPRESA (PREFERENTEMENTE)

No lo compartas con otras personas en el hogar, especialmente menores

CONECTATE USANDO VPN

Si no lo tienen implementado al menos evita utilizar WIFI públicas o compartidas con desconocidos

HackLabGirls Latam

TELETRABAJO ¿SEGURO?

Ciberconsejos para #quedarteEnCasa

EXTREMA PRECAUCIONES ANTE PHISHING

No abras adjuntos no solicitados o sospechosos.

RESPALDA PERIÓDICAMENTE

Los dispositivos de respaldo deben estar desconectados de tu equipo durante el uso rutinario para evitar daño masivo por ransomware

ES UN APORTE DE
#HACKLABGIRLS LATAM
#QUEDATEENCASA #CORONAVIRUS

EDI SAFE POLIS CAPSI EX CYBER PROJECT feyce HackLabGirls IT SERVICE & BEHAVING SecPro AW-ITC Grupo Jurídico HONDURAS Ciberseguro CISO's

Protege tu equipo y dispositivos móviles con credenciales de acceso y diferencia tus cuentas personales de las profesionales. Utilizar contraseñas robustas y el doble factor de autenticación.

«algo que sé», «algo que tengo» «algo que soy». **Autenticación de doble (o triple) factor**.

- Técnicas de autenticación externas
- No utilizar las contraseñas por defecto
- Doble factor para servicios críticos
- No compartir las contraseñas con nadie
- Las contraseñas deben de ser robustas
- No utilizar la misma contraseña para servicios diferentes
- Cambiar las contraseñas periódicamente.
- No hacer uso del recordatorio de contraseñas
- Utilizar gestores de contraseñas

Conclusiones

- Protege tu equipo y tus dispositivos móviles con credenciales de acceso.
- Diferencia tus cuentas personales de las profesionales. Recuerda utilizar siempre contraseñas robustas y el doble factor de autenticación siempre que sea posible.
- Mantén los **sistemas operativos y las aplicaciones actualizados**
- Trabajar en conexiones a internet seguras y protegidas. Evita uso de aplicaciones de acceso remoto, usa VPN red privada virtual
- Cifra tus soportes de información
- Protege tus datos. Realiza copias de respaldo periódicas.
- Evitar instalar aplicaciones de CODIV-19. Se ha convertido en plataforma sospechosa

Que se te meta en la cabeza

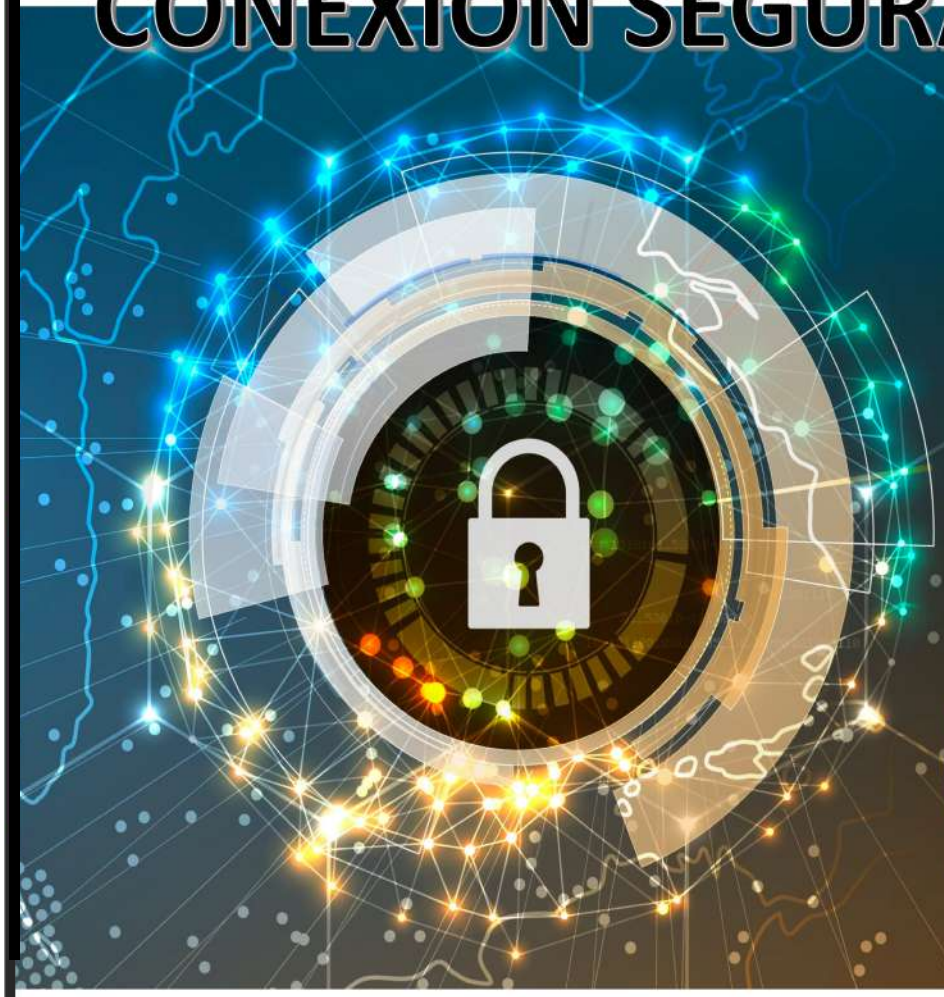
MSc. Ing. M. Angélica Castillo Ríos
angelica.castillorios@gmail.com
+51 975771442

Conferencia 2 de 11

Gustavo Guzmán

Académico y especialista en Gobierno de TI
y Ciberseguridad
Líder y parte del Comité de Expertos COLADCA
Capítulo México

CONEXIÓN SEGURA



INTEGRIDAD

CONFIDENCIALIDAD

DISPONIBILIDAD

Gustavo Guzmán está compartiendo una aplicación.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

CONEXIÓN SEGURA

- Política de SI
- Autenticación
- VPN
- Cultura de SI

Gustavo Guzmán

CONEXIÓN SEGURA

La CIBERSEGURIDAD es responsabilidad de todos.

"Si crees que únicamente la tecnología puede solventar tus problemas de seguridad, entonces no entiendes los problemas y no entiendes de tecnología".

Bruce Schneier

Conferencia 3 de 11

Nazly Borrero

Gerente IT Service & Beratung | Directora de la ORG Colombia Cibersegura
Líder y parte del Comité de Expertos COLADCA
Capítulo Colombia

BUENAS PRÁCTICAS APLICADAS AL USO DE LA TECNOLOGÍA

- Revise su conexión a internet
- Acceso remoto a información corporativa
- Asegure los equipos de cómputo

IT SERVICE & BERATUNG

Nazly Borrero está compartiendo una aplicación.

PRÁCTICAS DEL EMPLEADO SEGURO EN SU HOGAR

- Políticas de seguridad: acatar las políticas de seguridad de la organización aun estando fuera de la oficina.
- Dispositivos móviles: proteger los dispositivos móviles utilizados en el hogar para acceder a la red o información corporativa.
- Soluciones contra malware: si se emplea una computadora personal se deben utilizar, en la medida de los posible, los mismos controles de seguridad descritos en las políticas de seguridad de la organización.
- Actualizaciones de seguridad: las actualizaciones no solo incluyen mejoras en las funcionalidades, sino también parches de seguridad que corrigen fallas en los programas.

IT SERVICE & BERATUNG

Conferencia 4 de 11

CR (RP) Fredy Bautista García

Consultor Programa SAFE CCIT

Director Centro Cibernético Policial Años 2002 a 2018

CONFERENCIA 4 DE 11

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

CR RP FREDY BAUTISTA G está compartiendo una aplicación.

SAFE – SEGURIDAD APLICADA AL FORTALECIMIENTO DE LAS EMPRESAS

SAFE

- Mayor dependencia de la infraestructura digital
- Cibercrimen explota el miedo e incertidumbre
- Más tiempo en línea podría llevar a comportamientos riesgosos.

CR RP FREDY BAUTISTA G está compartiendo una aplicación.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

Alerta Global de Ciberataques y otros delitos

SAFE – SEGURIDAD APLICADA AL FORTALECIMIENTO DE LAS EMPRESAS

SAFE

Conferencia 5 de 11

David Pereira

CEO SecPro Security Professionals
Aliado y Parte del Comité de Expertos COLADCA

David Pereira está compartiendo una aplicación.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

CIBERSEGURIDAD AL ALCANCE DE TOD@S

DAVID PEREIRA

SecPro

David Pereira | Secpro

SecPro

Recomendaciones

Administradores de TI:

- ✓Proteger los Servicios de VPN
  - ✓ACL
  - ✓Rutas
  - ✓Aseguramiento DNS
  - ✓Filtrado de Tráfico
- ✓Pruebas de Carga y Stress
- ✓Estar Preparados para Ataques DoS/DDoS

Recomendaciones

SecPro

Cómo me protejo en línea?

- ✓Manejando la seguridad de mi Estación de Trabajo
- ✓Manejando mi privacidad
- ✓Garantizando mi Privacidad
- ✓Ya estoy hackead@?

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

Recomendaciones

SecPro

Mis Contraseñas - Autenticacion Multifactor

- ✓Errores Comunes
- ✓Contraseñas seguras
- ✓Gestores de Claves
- ✓Activar Autenticación Múlti Factor

David Pereira | Secpro

Recomendaciones

SecPro

Cómo protejo mis dispositivos?

- ✓PC (Windows)
  - ✓Herramientas de protección
  - ✓Actualizaciones
  - ✓Cifrado del Disco
  - ✓Cifrado de Archivos
  - ✓Borrado Seguro
- ✓Celulares / Tabletas (Android / IOS)
- ✓ Memorias USB

WEBINAR

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

Recomendaciones

SecPro

El Correo electrónico

- ✓Proteccion del Correo
- ✓Cifrado del Correo (PGP)
- ✓Detectando el Engaño

David Pereira | Secpro

Recomendaciones

SecPro

Las redes Inalámbricas

- ✓Limitar cantidad de Dispositivos
- ✓Clave ROBUSTA
- ✓No usar WiFi Públicos en lo posible

WEBINAR

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

Recomendaciones

SecPro

Uso Seguro de las Nubes

- ✓One Drive
- ✓Google Docs
- ✓Dropbox

David Pereira | Secpro

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

"Las Personas son la Primera Linea de Ciberdefensa"

DAVID PEREIRA

SecPro

David Pereira | Secpro

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

”Si somos conscientes del riesgo, estaremos alerta ante pontenciales ataques”

“Tu eres la primera línea de defensa de la Empresa y de tu Familia”

David Pereira | david.pereira@secpro.org

www.secpro.org

@d4v1dp3r31r4

SecPro

https://www.youtube.com/user/dfpluc2

David Pereira | Secpro

Conferencia 6 de 11

Andres Ricardo Almanza

CGO CISOS CLUB

Aliado Estratégico COLADCA

CONFERENCIA 6 de 11

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

Andres Almanza (CISOS.CLUB) está compartiendo una aplicación.

CISO's Club

DECÁLOGO DE HUMANIDAD Y SEGURIDAD PARA TRABAJAR EN EL MUNDO DIGITAL A TRAVÉS DEL TELETRABAJO

CISO's Club

www.cisos.co #LSD #LíderSegDigital. #Crecer #Cocrear #Contribuir #DesReAprender #Experimencias #Diflexión www.cisos.club

Andres Alma...

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

REFLEXIONES PARA EL LÍDER DE SEGURIDAD DIGITAL

CISO's

El entrenamiento de un #LSD para crear Seguridad de Alto Nivel

Ciber-Seguridad empieza con las PERSONAS y termina con las PERSONAS

Molécula de la Ciber-Seguridad

Cyber-Security Molecule

Cyber-Security start with People/Human and end with People/Human

www.cisos.co #LSD #LíderSegDigital. #Crecer #Cocrear #Contribuir #DesReAprender #Experimencias #Diflexión www.cisos.club

Andres Alma...

SEGURIDAD Y HUMANIDAD EN TIEMPOS DE CRISIS

CISO's

Decálogo de buenos hábitos

Rutina — Tener los mismos hábitos cotidianos

Acciones — Ejecutar las mismas actividades

Método — Dividir el día
- Mañana
- 90-10
- 60-10
- Almuerzo
- Tarde
- 60-10
- 60-10

Alimentación — Nutrición (Energía)

Reflexión — A la tarde

Espacio de trabajo — NO CAMA

Herramientas
- Equipo
- Email
- Browser
- Otros

Navegación
- Sin control
- Con control

Capacidades
- Responsabilidad
- Ética
- Empatía
- Inteligencia digital
- Gestión emocional digital
- Comunicación
- Equipos
- Adaptabilidad/Flexibilidad

Innovación/ Creatividad
- Propio
- Oficina

www.cisos.co #LSD #LíderSegDigital. #Crecer #Cocrear #Contribuir #DesReAprender #Experimencias #Diflexión www.cisos.club

SEGURIDAD Y HUMANIDAD EN TIEMPOS DE CRISIS

Decálogo de buenos hábitos

CISO's Club

SERÁ EL MOMENTO PARA SABER SI NUESTROS PROGRAMAS DE CULTURA DE SEGURIDAD DIGITAL NECESITAN SER REPENSADOS

www.cisos.co #LSD #LíderSegDigital. #Crecer #Cocrear #Contribuir #DesReAprender #Experimencias #Diflexión www.cisos.club

Andres Almanza (CISOS.CLUB) está compartiendo una aplicación.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

SEGURIDAD Y HUMANIDAD EN TIEMPOS DE CRISIS

Decálogo de buenos hábitos

CISO's

¿QUÉ SE NECESITA HACER DISTINTO PARA CREAR CULTURA DE SEGURIDAD DIGITAL ?

¿QUÉ SE NECESITA DEJAR DE HACER PARA CREAR CULTURA DE SEGURIDAD DIGITAL ?

¿A QUÉ TENDREMOS QUE RENUNCIAR PARA ENFRENTAR ESTOS NUEVOS DESAFÍOS EN EL MUNDO DE LA SEGURIDAD DIGITAL?

www.cisos.co #LSD #LíderSegDigital. #Crecer #Cocrear #Contribuir #DesReAprender #Experimencias #Diflexión www.cisos.club

Andres Alma...

Conferencia 7 de 11

Emanuel Ortiz

Director de la Asociacion internacional de informatica forense (ASIIF)
Y de la Red de investigación académica en Ciberseguridad y Cibercriminilogia (Red ciber)
Aliado Estratégico COLADCA

CONFERENCIA 7 de 11

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

Emanuel ortiz #2 está compartiendo una aplicación.

Tecnicas de SpearPhishing

Guia de Supervivencia ante la Ingenieria Social

Aprende cuales son las principales modalidades

ASOCIACION INTERNACIONAL DE INFORMATICA FORENSE (ASIIF)
RED DE INVESTIGACIÓN ACADEMICA EN CIBERSEGURIDAD Y CIBERCRIMINILOGIA (RED CYBER)

Emanuel orti...

Emanuel ortiz #2 está compartiendo una aplicación.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

Envío de Correos Electrónicos parte 1

El CIberdelincuente puede enviar correos engañosos al destinatario previa perfilación del usuario por medio de fuentes abiertas e internet para la obtención de información.

Señuelos

Los señuelos o formas de contacto pueden tratarse de una citación judicial, pago de impuestos etc...

#BEC: Business Email Compromise

Emanuel orti...

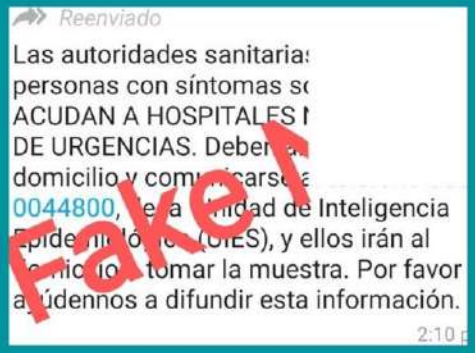
Emanuel ortiz #2 está compartiendo una aplicación.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

Envío de mensajes asociados a campañas

El CIberdelincuente puede utilizar mecanismos de engaño que permitan aprovecharse de algún aspectos sociales o coyuntura política, económica o de salud relacionada. Ej. COVID 19



Estan estructurados para cadenas de mensajes llamados hoax y provocar acceso a los datos personales

★★★★★

#NosigolaCadena

Emanuel orti...

Emanuel ortiz #2 está compartiendo una aplicación.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

Envío de Correos Electrónicos parte 2

El CIberdelincuente puede utilizar servicios para poder generar mensajes electrónicos de manera masiva y aleatoria a diferentes direcciones de correo electrónicas con el fin de engañar al usuario final.


La salud es de todos | Minsalud

Estimado ciudadano

Hemos intentado comunicarnos via telefonica con usted en el dia de hoy pero ha sido imposible , se trata de un tema muy delicado el cual le relatamos a continuación

Detectamos en su sector la presencia de COVID-19 (Corona virus) es por eso que como medida preventiva hemos adjuntado los sitios en los cuales no le recomendamos visitar ya que estos se encuentran a pocos metros de su residencia

Los señuelos o mensajes pueden estar relacionados con campañas realizadas por el Gobierno o ministerios.

★★★★★

#SeguridadenlaInformación

Emanuel orti...

Top 10 de asuntos de Ingenieria Social

Infografia CSIRT 003

El Csirt Financiero previene al Sector sobre los asuntos más usados en las campañas de Phishing y SpearPhishing en Colombia.

1. "Embargo bancario"
2. "Tenemos un problema Financiero con su cuenta"
3. "Citación Fiscalia General de la Nación"
4. "Reporte de Fraude desde su Dirección IP"
5. Fiscalia proceso 305431T
6. "Proceso Pendiente Migración Colombia"
7. "Detalles de su cuenta"
8. " Cancelación de Cedula"
9. "Su Ip está reportada en un Crimen"
10. "Te han enviado un mensaje Privado"

#Covid19

ANÁLISIS DE Z5HKgyhqPT.jar

Imagen 1: Análisis de comportamiento del malware

MITRE ATT&CK

Imagen 8: Análisis MITRE ATT&CK

TTP

1. Debilidades en el sistema de archivos
2. Deshabilitado herramientas de seguridad
3. DLL Side - Loading
4. Ofuscación de archivos
5. Descubrimiento

Conferencia 8 de 11

Juan David Cardona

Director Estratégico Arcont Group SAS
Aliado Estratégico COLADCA

CONFERENCIA 8 de 11

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

"El TELETRABAJO, Y SUS RIESGOS LABORALES", desde una perspectiva mixta, vinculando las TIC's al Derecho.

Juan David Cardona Pérez

Director Estratégico

mail: juan.cardona@arcontgroup.com

Cel: +57 3185455603

ARCONT GROUP S.A.S

JUAN DAVID CARDONA está compartiendo una aplicación.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

JUAN DAVID CARDONA PÉREZ

CIBERABOGADO

www.arcontgroup.com

Juan.Cardona@arcontgroup.com

- Director Estratégico de la compañía Arcont Group s.a.s. Abogados y soluciones técnicas forenses
- Vicepresidente en The International Association Identification "IAI" División Colombia.
- Consultor para Telemundo internacional, en el programa al rojo vivo en temas digitales y ciber.
- INGENIERO DE SISTEMAS. Especialista en seguridad informática.
- Especialista en informática forense (Identificación, Recolección, preservación, análisis y preservación de la evidencia digital).
- ABOGADO, Maestrando en Derecho de la Ciberseguridad y Entorno Digital, en la Universidad de León España.
- Magister en Derechos Humanos DDHH y Derecho Internacional De Los Conflictos Armados DICA.
- Docente universitario, Conferencista, analista y consultor en temas ciber.

® Todos los de

us.bbcollab.com comparte tu pantalla y audio. Dejar de compartir Ocultar

lo 16-79 oficina 404 torre B , CC Expocentro

En Colombia, Ley 1221 de 2008 establece tres modalidades de

4. Las medidas de seguridad informática que debe conocer y cumplir el teletrabajador.

las tareas a ejecutar y el perfil del trabajador.

Teletrabajo Suplementario

Teletrabajo Autónomo

Teletrabajo Móvil

DECRETO 884 /2012, por medio del cual se regula ciertos aspectos de la Ley 1221 de 2008.

1. Las condiciones de servicio, los medios tecnológicos y de ambiente requeridos y la forma de ejecutar el mismo en condiciones de tiempo y si es posible de espacio.
2. Determinar los días y los horarios en que el teletrabajador realizará sus actividades para efectos de delimitar la responsabilidad en caso de accidente de trabajo y evitar el desconocimiento de la jornada máxima legal.
3. Definir las responsabilidades en cuanto a la custodia de los elementos de trabajo y fijar el procedimiento de la entrega por parte del teletrabajador al momento de finalizar la modalidad de teletrabajo.
4. Las medidas de seguridad informática que debe conocer y cumplir el teletrabajador.

JUAN DAVID CARDONA está compartiendo una aplicación.

JUAN DAVID CARDONA está compartiendo una aplicación.

JUAN DAVID CARDONA está compartiendo una aplicación.

RIESGOS CIBERNÉTICOS

RIESGOS PSICOSOCIALES

RIESGOS FISICOS

RIESGOS LEGALES

Conferencia 9 de 11

Carlos Castañeda M. PhD

Consultor Feyce Integrales SAS | Investigador en Ciberseguridad y Ciberdefensa
Asociado a la Escuela Superior de Guerra “General Rafael reyes Prieto”
Aliado Estratégico COLADCA

CONFERENCIA 9 de 11

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

Carlos Castaneda - EFEYCE #2 está compartiendo una aplicación.

Nivel Madurez para la contingencia en la pequeña y gran empresa

Carlos A. Castañeda M. PhD

Carlos A. Castañeda M.
Carlos.castaneda@efeyceintegrales.com
Carrera 9 No. 61 - 77 Ofc. 201
+57 (1) 3100791
Cell 3167429975

EFEYCE Integrales SAS
info@efeyceintegrales.com
www.efeyceintegrales.com
Carrera 9 No. 61 - 77 Ofc. 201
+57 (1) 3100791

Carlos Castaneda - EFEYCE #2 está compartiendo una aplicación.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

El 60% de las pequeñas y medianas empresas, no pueden sostener sus negocios más de seis meses luego de sufrir un ciberataque importante.
Ésto demuestra que los factores en torno a los Ciberataques a PYMES en Colombia comprometen seriamente los activos económicos e impactan asuntos estrictamente legales y de cumplimiento de las compañías.

60%
PYMES

Informe de las tendencias del cibercrimen en Colombia (2019 -2020) - Policía de Nacional de Colombia

Ejemplo de una cadena de "hackeo" (Cyber Kill Chain)

- Los ataques internos son los que normalmente generan mas daños.
- Los movimientos maliciosos "Left of the Hack" son los más difíciles de detectar.
- Los movimientos maliciosos "Right of the Hack" son los que dejan consecuencias graves para el negocio.

Carlos Castaneda - EFEYCE #2 está compartiendo una aplicación.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

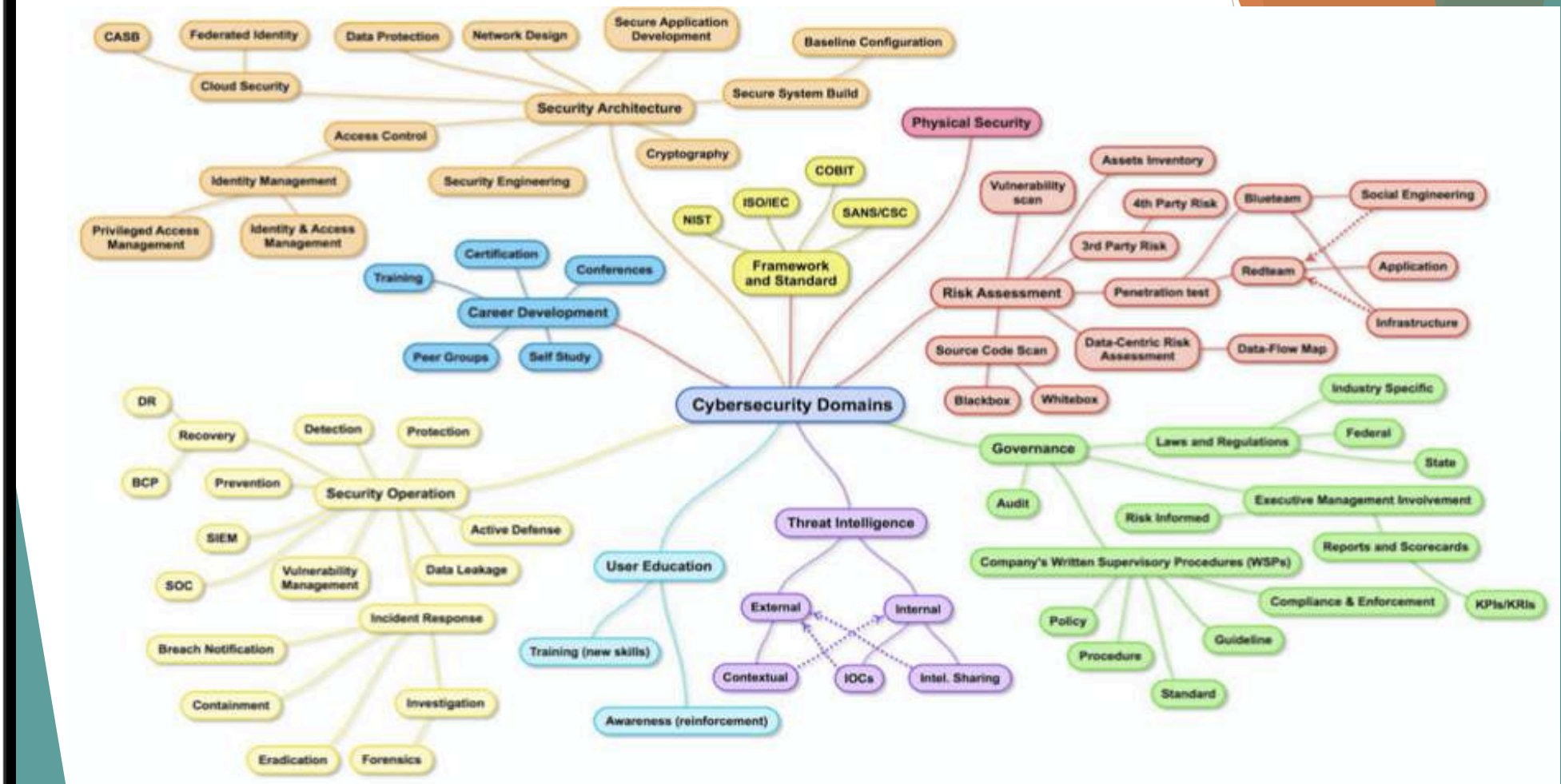
WEBINAR

"La información es el activo más importante de las organizaciones. La seguridad por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados"

Carlos Castaneda - EFEYCE #2 está compartiendo una aplicación.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR



INFORMACIÓN

- Dónde está?
- Quién Accede?
- Cuándo?
- Control / monitoreo?
- Disponibilidad

Carlos Castaneda - EFEYCE #2 está compartiendo una aplicación.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

Vectores de Ataque en el tiempo de la pandemia

- Suplantación de usuarios
- Robo de credenciales
- Ingenieria Social
- Correo Electróinico - Phishing
- Propagación de virus y ramsomware

Recomendaciones Iniciales (Capacidad de Resiliencia)

- Gestión de la identidad de los usuarios.
- El usuario es el centro de la seguridad
- **Campaña recurente de concienciación para los usuarios.**
- Activar y probar el Plan de Continuidad de Negocio. DRP y Backup.
- Revisar el conjunto mínimo de herramientas que permitan la visibilidad de la actividad en la red.
- Control de la Cloud
- Política del menor privilegio.
- Monitoreo activo de todo y en especial el acceso VPN

Conferencia 10 de 11

Ana Maria Mesa Elneser. PhD

Directora y fundadora de Law TIC Grupo Jurídico
Representante para Colombia de la RED EDI
Enlace del Convenio de Cooperación Interinstitucional COLADCA con la Facultad de Derecho de la Universidad UNAULA | Universidad Autónoma Latinoamericana
Líder y parte del Comité de Expertos COLADCA

CONFERENCIA 10 de 11

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

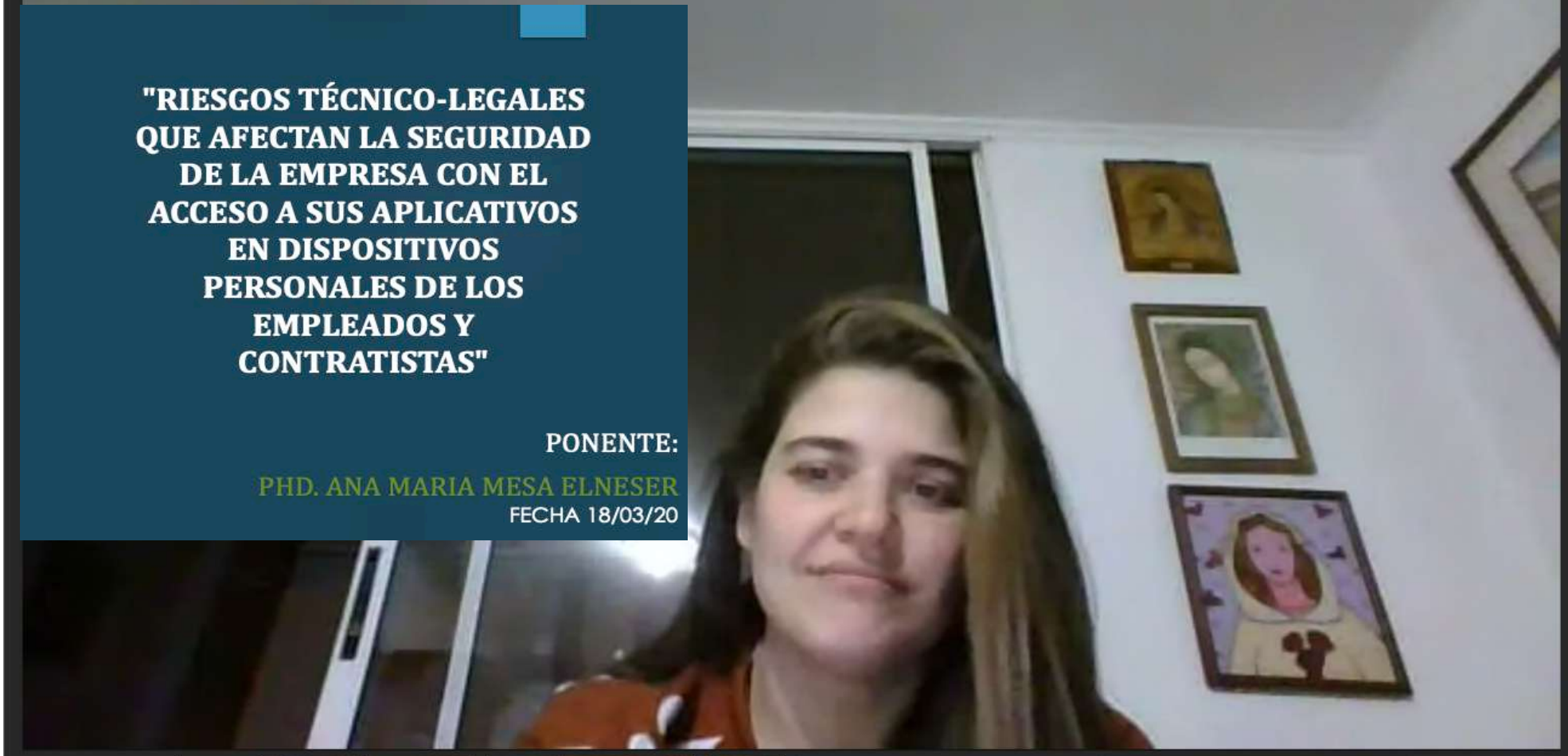
WEBINAR

"RIESGOS TÉCNICO-LEGALES QUE AFECTAN LA SEGURIDAD DE LA EMPRESA CON EL ACCESO A SUS APLICATIVOS EN DISPOSITIVOS PERSONALES DE LOS EMPLEADOS Y CONTRATISTAS"

PONENTE:

PHD. ANA MARIA MESA ELNESER

FECHA 18/03/20



JUAN DAVID C...
Presentador

¡Contáctenos!

IAW-ITC Grupo Jurídico

lawtic info@lawtic.com.co

313 7472426 - 317 7420405 318 7887582

www.lawtic.com.co

Seguridad Digital y Ciberseguridad
en Jornadas de Teletrabajo

TELETRA BAJO O TRABAJO EN CASA

¿Qué aspectos ponen en jaque la ciberseguridad de la empresa?

LAW – TIC
Grupo Juridico

Coherencia Técnico-legal

Elección de herramientas tecnológicas que cuenten con funcionalidades de seguridad por el proveedor o *in house*

Reglamentar el uso de herramientas tecnológicas desde Políticas, reglamentos, contratos, acuerdos, instrucciones del propietario de la herramienta

Adoptar controles técnicos y legales para el procesamiento y tratamiento de datos he información

DATOS/INFORMACIÓN empresa

HERRAMIENTA empleado

LAW-TIC Grupo Jurídico

ENTORNO DE LA PERSONA NATURAL Art. 15

PRIVACIDAD COMO DERECHO CONTRACTUAL

LAW-TIC Grupo Juridico

INTIMIDAD - PRIVACIDAD

ART. 15 C. Pol

"Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar."

Corte Constitucional SU-056 de 1995

Lo íntimo, lo realmente privado y personalísimo de las personas es, como lo ha señalado en múltiples oportunidades esta Corte, un derecho fundamental del ser humano, y debe mantener esa condición, es decir, pertenecer a una esfera o a un ámbito reservado, no conocido, no sabido, no promulgado, a menos que los hechos o circunstancias relevantes concernientes a dicha intimidad sean conocidos por terceros por voluntad del titular del derecho o por que han trascendido al dominio de la opinión pública.

Corte Constitucional, en Sentencia T-696 de 1996

La intimidad, el espacio exclusivo de cada uno, es aquella órbita reservada para cada persona y de que toda persona debe gozar, que busca el aislamiento o inmunidad del individuo frente a la necesaria injerencia de los demás, dada la sociabilidad natural del ser humano.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

WEBINAR

INTIMIDAD - PRIVACIDAD

Corte Constitucional, en Sentencia T-696 de 1996

El uso del correo electrónico e Internet en las empresas ha abierto un nuevo capítulo en el debate sobre los límites de la privacidad y el control. Es claro que se minimizan los conflictos en una empresa por aspectos relacionados con el correo-e cuando las empresas disponen de políticas de uso sencillas, claras y conocidas por todos.

Sentencia T-530 de 23 de septiembre de 1992

El núcleo esencial del derecho a la intimidad define un espacio intangible, inmune a intromisiones externas, del que se deduce un derecho a no ser forzado a escuchar o a ver lo que no se desea escuchar o ver, así como un derecho a no ser escuchado o visto cuando no se desea ser escuchado o visto.

Corte Constitucional, T-349 de 27 de agosto de 1993

"... derecho individual resultado del status libertatis de la persona, que, como ya se dijo, garantiza a ésta un espacio inviolable de libertad y privacidad frente a su familia, a la sociedad y al Estado. La inviolabilidad de la correspondencia es apreciada en cuanto preserva el derecho de la persona al dominio de sus propios asuntos e intereses, aún los intranscendentes, libre de la injerencia de los demás miembros de la colectividad y, especialmente, de quienes ejercen el poder público."

LAW-TIC Grupo Jurídico

Colombia Cibersegura · EDI · SAFE · POLIS · CAPSI · Ex Cyber Project · Feyce · HackLabGirls · IT Service & Beating · SecPro · LAW-TIC Grupo Jurídico · Honduras Cibersegura · CISO's

Seguridad Digital y Ciberseguridad
en Jornadas de Teletrabajo

TELETRA BAJO O TRABAJO EN CASA

"Debemos adoptar criterios y estrategias legales para mitigar, controlar o eliminar al impacto negativo derivado del riesgo en entornos digitales!

REGLAMENTACIONES OBLIGATORIAS

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

Reglamento Interno de Trabajo

1. Obligaciones y responsabilidades en las herramientas informáticas del empleador
2. Limitaciones de uso de herramientas para uso personal
3. Causal de sanción leve o grave

Contrato de trabajo y prestación de servicios

1. Contrato de trabajo escrito con acuerdo de confidencialidad y limitaciones en el uso de información y datos, sean personales o impersonales
2. Contrato de prestación de servicio con acuerdo de confidencialidad y acuerdo de protección de datos personales

Parte interesada interna y externa

1. Comunicar permanentemente
2. Capacitar en ciclos periódicos
3. Formar en áreas críticas y de forma permanente.

REGLAMENTACIONES OBLIGATORIAS

LEY 1581 DE 2012

1. Implementar el manual de protección de datos
2. Establecer políticas de seguridad de la información que preserven los riesgos físicos y lógicos respecto de los datos e información
3. Garantizar en todo tiempo los principios de: seguridad, acceso y circulación restringida, confidencialidad.
4. Establecer guía de levantamiento de información del incidente y generación de tratamiento del riesgo para la construcción del informe para reporte a titulares y la SIC

LAW-TIC Grupo Jurídico

Colombia Cibersegura · EDI · SAFE · POLIS · CAPSI · Ex Cyber Project · feyce · HackLabGirls · IT Service & Beating · SecPro · LAW-TIC Grupo Jurídico · Honduras Cibersegura · CISO's

REGLAMENTACIONES OBLIGATORIAS

ISO 27001:2013
ANEXO A

A.6.2. Dispositivos Móviles y Teletrabajo.
Objetivo. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

A.6.2.1. Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

A.6.2.2. Teletrabajo. Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

ISO 27001:2013
ANEXO A

A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.

A.7.1. Antes de asumir el empleo.
Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

A.7.1.1. Selección. Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

A.7.1.2. Términos y condiciones del empleo. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.

REGLAMENTACIONES OBLIGATORIAS

ISO 27001:2013
ANEXO A

A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.

A.7.2. Durante la ejecución del empleo.
Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

A.7.2.1. Responsabilidades de la Dirección. La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.

A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información. Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

A.7.2.3. Proceso disciplinario. Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

REGLAMENTACIONES OBLIGATORIAS

ISO 27001:2013
ANEXO A

A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.

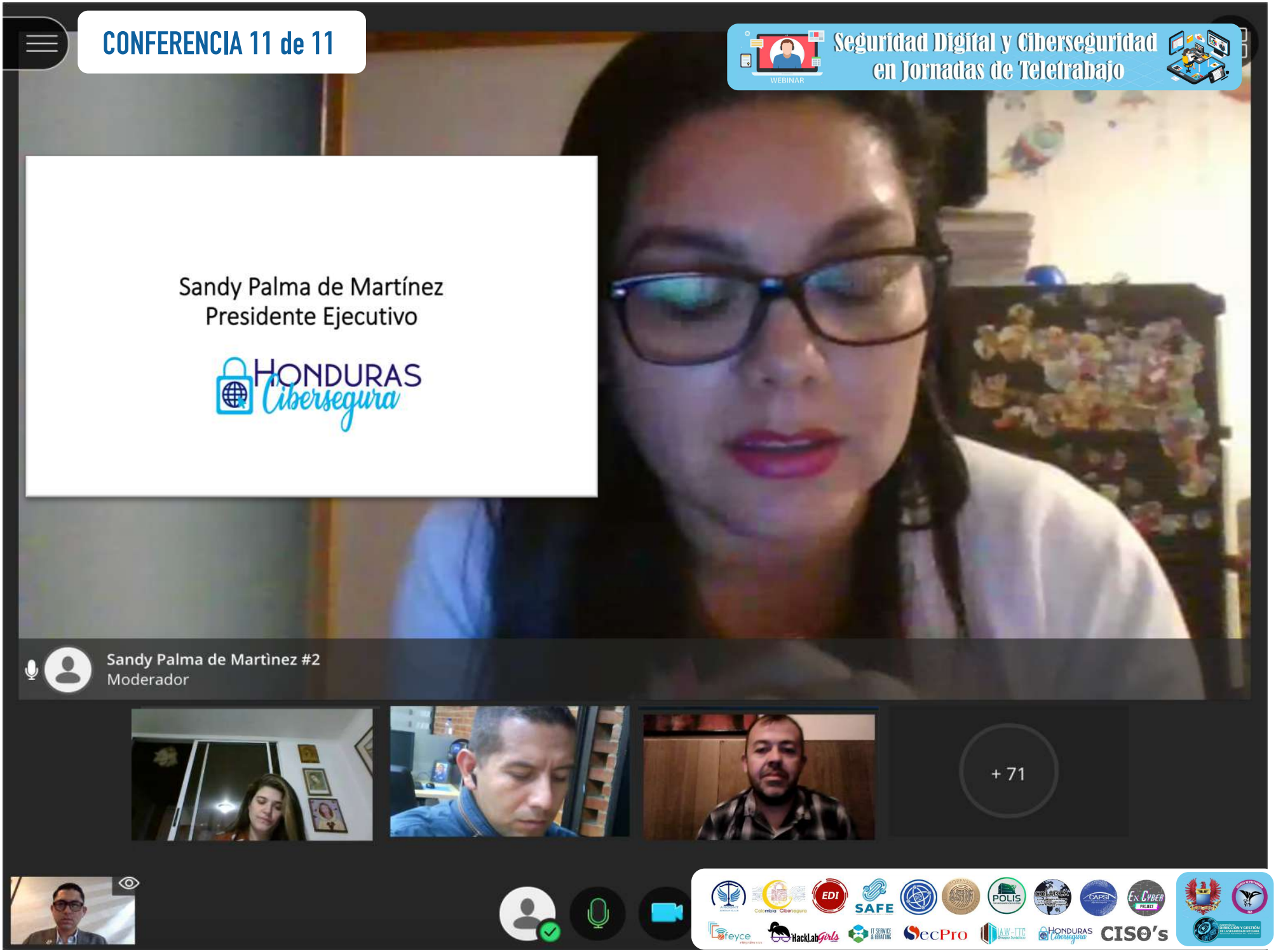
A.7.3. Terminación y cambio de empleo.
Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

A.7.3.1. Terminación o cambio de responsabilidades de empleo. Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.

Conferencia 11 de 11

Sandy Palma de Martínez

Presidente Ejecutivo de la ORG Honduras Cibersegura
Jefe de la Unidad de Transparencia y Acceso a la Información Pública
de la Secretaría de Gobernación, Justicia y Descentralización en Gobierno de Honduras
Líder y parte del Comité de Expertos COLADCA
Capítulo Honduras


CONFERENCIA 11 de 11
WEBINAR
Seguridad Digital y Ciberseguridad
en Jornadas de Teletrabajo
Sandy Palma de Martínez
Presidente Ejecutivo
HONDURAS
Cibersegura
Sandy Palma de Martìnez #2
Moderador
+ 71
EDI
SAFE
POLIS
CAPSI
HackLabGirls
SecPro
HONDURAS Cibersegura
CISO's

Uso de redes WiFi seguras

Recordar a los empleados que solo trabajen en conexiones a Internet seguras y protegidas con contraseña. Si tiene que usar WiFi públicas, es necesario asegurarse de verificar con el propietario que la red a la que se está conectando es su red legítima y está protegida mediante cualquier otro tipo de mecanismos. Evite acceder a información confidencial desde una red WiFi pública.

Recuerde a los empleados que no deben usar laptops personales para trabajar

Solicite a sus empleados que usen computadoras portátiles suministrados por la entidad o que se comuniquen con el personal de seguridad de la información si necesitan soporte y aseguramiento sobre el equipo que están utilizando. El uso de dispositivos personales crea problemas relacionados con la preservación de documentos y agrega un mayor riesgo. Además, el software instalado en algunos equipos domésticos puede estar desactualizado durante meses o incluso años.

Gestión de información confidencial

Recuerde a los empleados que usen la misma atención o incluso con mayor rigor sobre la información confidencial como lo harían si estuvieran en la oficina. El correo electrónico personal **no debe utilizarse** para ningún negocio de la empresa, y los empleados deben realizar un seguimiento de lo que están imprimiendo en casa. Implemente controles de impresión, copiado y modificación sobre aquella información que considere altamente confidencial.

Contactos y canales de emergencia

Asegúrese de que su entidad adopte mecanismos "fuera de línea" para contactar a todos los empleados, ya sea un número de teléfono celular u otra forma de contactar al empleado fuera de los sistemas de la entidad. De esa manera, si la entidad es víctima de un ataque (malware, rescate, DDoS u otro tipo), podrá comunicarse con sus empleados. Para el personal clave o la alta gerencia, configure un grupo en una aplicación segura de mensajes de texto como *Signal*, de modo que, si los sistemas no funcionan y el correo electrónico se encuentra indisponible, la alta gerencia podrá comunicarse sin temor a la intercepción de ciberdelincuentes.

HONDURAS Cibersegura

Gestión de información confidencial

Recuerde a los empleados que usen la misma atención o incluso con mayor rigor sobre la información confidencial como lo harían si estuvieran en la oficina. El correo electrónico personal **no debe utilizarse** para ningún negocio de la empresa, y los empleados deben realizar un seguimiento de lo que están imprimiendo en casa. Implemente controles de impresión, copiado y modificación sobre aquella información que considere altamente confidencial.

Infografía: Joshsua González - Colombia

Todo mundo preocupado por planes de contingencia de tecnología, ciberseguridad, estructuras críticas y demás y muchos no tomaron en cuenta el elemento más importante como son las personas... Ahora todos están queriendo reaccionar como puede sin estrategias de sucesión ni personal alterno....

Nadie o pocos reforzaron o contempló el teletrabajo... Ahora se está haciendo lo que se puede porque nadie está pensando en hackers crackers, fraudes, corrupción, etc.... Todo se está conectando a las redes que puede... Las universidades, colegios, empresas, grandes, pequeñas, casas..... Que esto nos sirva de experiencia de lección todos.... ***HAY QUE CAMBIAR LA MENTALIDAD...***

Mauricio Fiallos
ISACA Honduras Capitulo en Creación

Cierre Webinar

Capitán Yuber Rico

Coordinador de la Maestría en Dirección y Gestión de la Seguridad Integral - MADGSI
Escuela de Postgrados de la Fuerza Aérea Colombiana – EPFAC
Aliado Estratégico COLADCA

Edgardo Glavinich

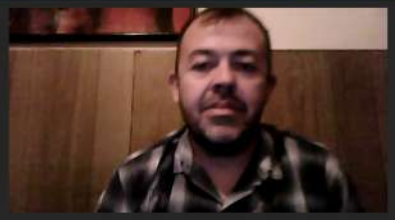
Secretario CAPSI
Camara Argertina de Profesionales en Seguridad Integrada
Aliado y Parte del Comité de Expertos COLADCA
Capitulo Argentina

CIERRE WEBINAR

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

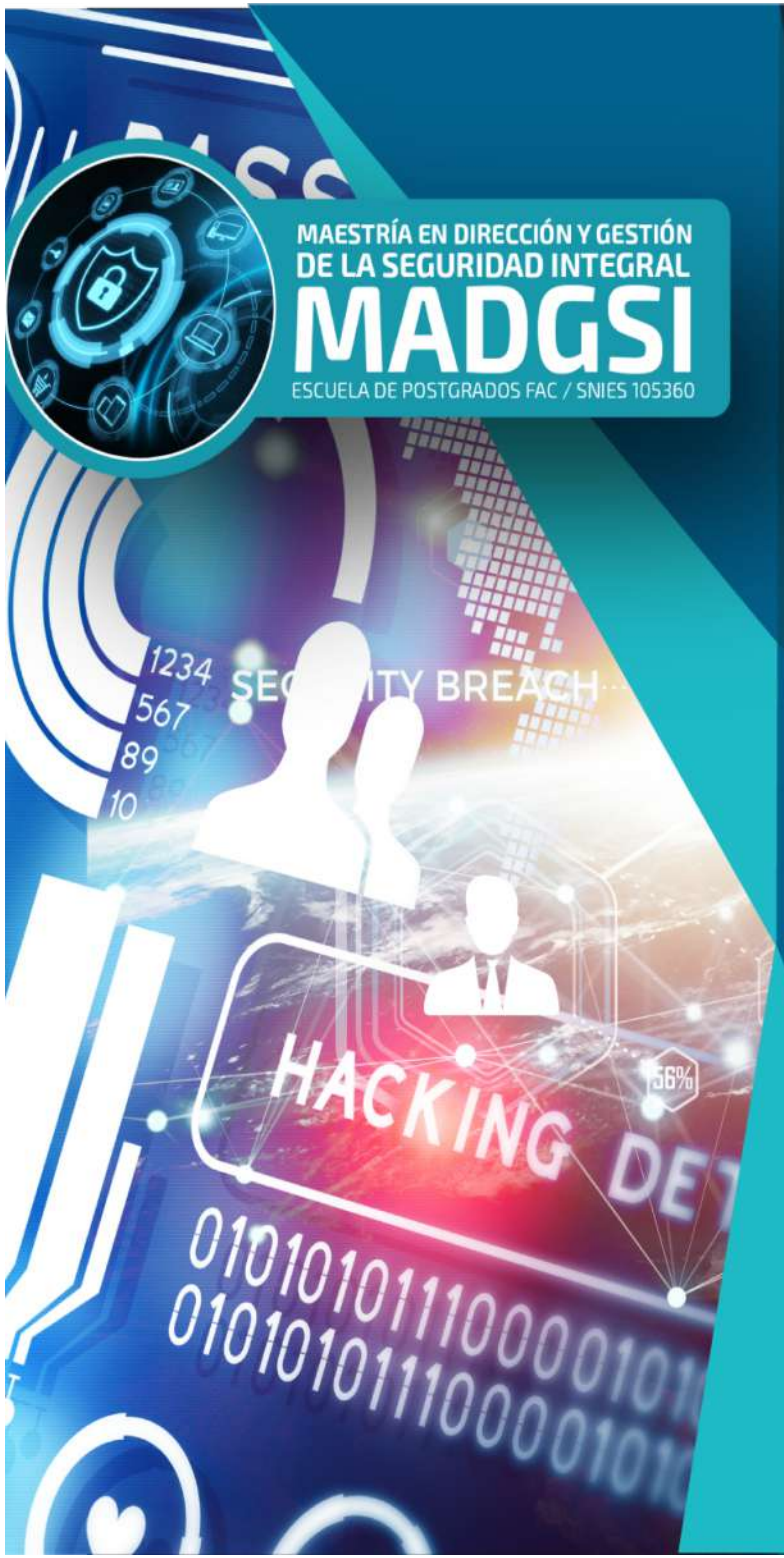
WEBINAR

CAPITÁN YUBER RICO – MAESTRIA EN DIRECCIÓN Y GESTIÓN DE LA SEGURIDAD INTEGRAL EPFAC – FUERZA AÉREA COLOMBIANA



EDGARDO GLAVINICH | SECRETARIO CAPSI – CAMARA ARGENTINA SEGURIDAD INTEGRAL

ARISTIDES CONTRERAS | PRESIDENTE COLADCA



MAESTRÍA EN

DIRECCIÓN Y GESTIÓN DE LA SEGURIDAD INTEGRAL

El programa de MADGSI tiene como propósito formar un magíster a través de un plan de estudios que integra conceptos, teorías, políticas, herramientas, procedimientos de dirección, gestión estratégica e investigación, capaz de construir conocimiento propio, gestionar procesos, diseñar sistemas de seguridad integral, tomar decisiones y resolver problemas que inciden en la operación, productividad, competitividad y resiliencia de las organizaciones para la protección de activos e infraestructuras críticas en el ámbito nacional, regional e internacional.

ESCUELA DE POSTGRADOS
FUERZA AÉREA COLOMBIANA
VIGILADA MINEDUCACIÓN

www.epfac.edu.co


COLADCA
Comunidad Latino Americana de Consultores y Asesores en Gestión de Riesgos y Seguridad
CAPSI
Cámara Argentina de Profesionales en Seguridad Integrada
COLADCA - CAPSI
La Comunidad COLADCA trabaja con su Aliado CAPSI Camara Argetina de Profesionales de Seguridad Integrada en un Nuevo modelo de Seguridad
4.0
SECURITY
¿Quiere mas o ser parte del Proyecto?
Déjenos saberlo
www.coladca.com | www.capsi-ar.org

Seguridad Digital y Ciberseguridad en Jornadas de Teletrabajo

Transmisión a través de:

Blackboard

RECUERDE! DEBE REGISTRARSE PARA MANTENER CONTACTO COLADCA Y SEGUIR SIENDO INVITADO A NUEVOS WEBINAR, USE EL LINK:

https://bit.ly/2IX7C3o

Sigamos "Dejando Huella"

COMUNIDAD COLADCA | www.coladca.com

ESCUELA DE POSTGRADOS
FUERZA AÉREA COLOMBIANA
VIGILADA MINEDUCACIÓN

MAESTRÍA EN
DIRECCIÓN Y GESTIÓN
DE LA SEGURIDAD INTEGRAL
ESCUELA DE POSTGRADOS FAC / SNIES 105360

Organizan y apoyan

Fecha: 18 de Marzo de 2020
Hora: 17:00 Hrs a 19:00 Hrs
(UTC-05:00) Bogotá, Lima, Quito

Cupo y Preregistro:
https://bit.ly/2IX7C3o