Guía de ciberseguridad para 2020 lo que necesitas tener en el radar

Reset
Una idea Bancolombia

Índice de contenidos

Introducción

¿Por qué la ciberseguridad es más importante ahora que nunca?

Seguramente porque es transversal a toda la revolución 4.0 que viven las industrias, las empresas y la sociedad en la actualidad.

El aumento del uso de tecnologías como: el Internet de las cosas (IoT por sus siglas en inglés), Inteligencia artificial, Big data, Cloud computing, Impresión 3D, entre otras, en los diferentes sectores económicos están generando dos principales riesgos: riesgos de seguridad y de privacidad de los datos, lo que ubica a la ciberseguridad en un nivel de relevancia alto y una prioridad.

Según datos del **informe**: Desafíos el riesgo cibernético en el sector financiero para Colombia y América Latina, se está haciendo la tarea frente a la protección y sensibilización de riesgos cibernéticos:

88%

de las entidades bancarias de la región han implementado tanto sistemas de detección/ prevención de intrusiones (IDS e IPS), como procesos de monitoreo de amenazas y vulnerabilidades.

88%

de los bancos ofrece un mecanismo para que sus usuarios internos (empleados y contratistas) reporten incidentes (ataques exitosos).

82%

de entidades bancarias cuenta con planes de preparación, respuesta y capacitación.

Y aunque las cifras son alentadoras sobre el trabajo que se viene realizando en ciberseguridad en Colombia y Latinoamérica, todavía hay mucho por hacer.

Por eso, **en esta guía de ciberseguridad 2020**, te contamos sobre los temas más sobresalientes que están amenazando la seguridad informática, tanto en el aspecto personal como empresarial.

Riesgos y amenazas que deben estar en el radar de todo profesional del sector financiero para seguir fortaleciendo no solo, los mecanismos y estrategias de seguridad, sino las campañas de sensibilización y autoprotección dentro del entorno laboral.

¡Comencemos!

1 Tendencias de ciberseguridad en 2020: 5 temas claves a monitorear

Eset Latinoamérica, empresa líder en seguridad de la información, a través de su blog, realiza un trabajo de contenido educativo e informativo bastante valioso.

Por eso, recurrimos a ellos en busca de respuestas a la pregunta ¿cuáles serán las tendencias en **ciberseguridad para 2020**?

- **Transformación digital dentro de las empresas y sus desafíos.**
- **Ciudades inteligentes.**
- **La Inteligencia artificial y Machine learning en la banca.**

- **Más Fake news y Deepfakes.**
- **Políticas y leyes de privacidad más detalladas.**

Presta mucha atención a este video y prepara la lupa para lo que será tendencia en materia de seguridad informática para este año.

Ver vídeo

De 5 temas relevantes nos habló el especialista de seguridad de Eset Latinoamérica, Luis Lubeck, para quien una regla de oro en el ciberespacio siempre será: comprobar la información en más de una fuente, ya que “cada día se vuelve más evidente que no todo lo que brilla es oro, ni que todo lo que leemos es verdad”.

1. Transformación digital dentro de las empresas y sus desafíos

El desafío en ciberseguridad en Colombia para la empresas y sus área de T.I. es grande.

Este año se refuerza la hiperconectividad de las que gozan las personas, a propósito de la implementación de la conexión 5G, así mismo entonces, deben reforzarse las medidas de seguridad interna como externa. ¿Cómo así que externa?

Con los **nuevos modelos laborales** como el teletrabajo y otras reestructuraciones de procesos que conlleva la transformación digital, las empresas se verán en la necesidad de implementar protocolos de seguridad de la información que cubran a los empleados que trabajan desde sus hogares, bibliotecas o cafés y que se estarán por lo mismo, más expuestos.

Por eso, el investigador Camilo Gutiérrez, en el **Informe de tendencias de ciberseguridad 2020, de Eset** recomienda:

> ***(...) Es importante que las empresas no sigan considerando la seguridad de manera clásica, sino que piensen en pasar a modelos adaptativos que puedan responder a los cambios”***

2. Ciudades inteligentes

A medida que las personas incrementan el uso de dispositivos IoT y que a su vez, edificios y ciudades los van acogiendo en sus infraestructuras y sistemas de funcionamiento, (sensores de iluminación, temperatura, accesos remotos), se hace urgente que así como se hacen inteligentes para brindar confort, lo sean también en temas de seguridad frente a ataques cibernéticos, por ejemplo, malwares como Jackware.

> ***“Se calcula que para 2025 habrá ya 74.440 objetos IoT a nivel global”***

¿Qué sucedería si un atacante consigue comprometer el sistema de automatización de un edificio inteligente y amenaza con tomar el control a cambio del pago de un rescate de varios miles de dólares? Se pregunta la investigadora de seguridad Cecilia Pastorino en su artículo: *De dispositivos IoT a edificios y ciudades inteligentes: Smart is the new sexy.*

"Aprende más sobre **Internet de las cosas (IoT)**, una tecnología revolucionaria que se impone para "cambiarnos el chip".

3. La Inteligencia artificial y Machine learning en la banca

Está claro que la evolución de esta tecnología y los desarrollos de la Inteligencia artificial en la industria, marketing y vida cotidiana nos tienen deslumbrados, los expertos advierten que también deben alertarnos sus alcances.

¿Qué pasa si el Machine learning se utiliza indebidamente para atacarnos a nosotros y a los sistemas que hemos creado? Se preguntan los investigadores de Eset.

Por esta razón, el llamado es a estar atentos frente a los alcances y riesgos que representa para la seguridad de la información y la veracidad de la misma.

Fuera del sector de la tecnología, la industria de servicios financieros es la que más gasta en servicios de inteligencia artificial y está experimentando un crecimiento muy rápido. Hasta hace poco, los fondos de cobertura y las firmas HFT eran los principales usuarios de IA en las finanzas, pero las aplicaciones ahora se han extendido a otras áreas, incluidos bancos, reguladores, Fintech, firmas de seguros, por nombrar algunos.

Dentro de la industria de servicios financieros, las aplicaciones de IA incluyen comercio algorítmico, composición y optimización de cartera, validación de modelos, back testing, robo-advising, asistentes virtuales de clientes, análisis de impacto en el mercado, cumplimiento normativo y pruebas de estrés.

La Inteligencia artificial y el machine learning sin embargo, están cambiando cambiando la industria de servicios financieros, a saber en la detección de fraude y cumplimiento; servicios bancarios de chatbots y robo advisory; y comercio algorítmico.

Mira un artículo de nuestro blog que puede alimentar más este debate.
¿Es clave la inteligencia artificial para combatir ataques informáticos?

4. Más Fake news y Deepfakes

Esta es una tendencia que se desprende del uso de Machine learning e Inteligencia artificial en actividades fraudulentas, que provocan manipulación de la opinión pública, desinformación y posibilidad de fraude a empresas y compañías.

> ***Según un informe del MIT, un fake news tiene un 70% más de viralización que una noticia convencional de un medio tradicional.***

Esto vaticina el especialista de seguridad de la información, Jake Moore, quien también hace parte del equipo de investigadores de Eset:

> *“Durante la próxima década veremos videos falsos que involucran a figuras públicas y que antes nos hubieran parecido inimaginables. Pero, además, con el tiempo veremos que estos videos incluirán a personas más cercanas a nosotros, como pueden ser colegas, compañeros o familiares, así como también que los ciberdelincuentes utilizarán esta tecnología para engañar a sus víctimas. Los deepfakes lograrán que algunos de nosotros incluso no confiemos en nada, por más que nuestros sentidos nos digan que estamos ante un contenido verdadero”.*

¿Cuál es el reto frente a este fenómeno? Usuarios más educados y críticos para determinar la veracidad de la información que consumen.

5. Políticas y leyes de privacidad más detalladas

Tres factores van a caracterizar esta tendencia.

- La mayor responsabilidad y conciencia de los usuarios a la hora de exponer o entregar sus datos personales.

- El manejo más sensible y ético, por parte de las empresas, de la información y datos que recopilan y obtienen de los usuarios.

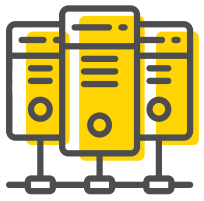
- La implementación de leyes y políticas como la GDPR (General Data Protection Regulation), que exijan a las empresas un mejor uso y protección de los datos personales que obtienen de sus usuarios. Y sanciones fuertes para quienes no las cumplan.

Recomendaciones de seguridad informática

Para finalizar, el especialista en seguridad, Luis Lubeck nos entrega una serie de recomendaciones para hacer frente a los retos de ciberseguridad que se presentarán durante 2020.

Y enfatiza, “el empleado del sector financiero, en cualquiera de las áreas, es el que tiene que estar más atento y alerta de la información que recibe o manipule de un medio digital. Son los más expuestos a ataques informáticos ”.

¿Qué hacer para prevenir ataques informáticos dentro de las empresas?



Ningún dispositivo o ninguna persona que esté conectada al ecosistema de la compañía, debe quedar por fuera de las políticas de seguridad de las empresas.

Las áreas de T.I. deben tener un rol más activo.

Verificar noticias o videos con fuentes confiables. La información debe ser reevaluada.

Sana paranoia y autoprotección.

Promover campañas de seguridad de la información y capacitaciones constantes frente al tema.

2 Ciberseguridad: un asunto de conciencia y cultura, un asunto de todos

En una nota de la revista Dinero se informa que en un estudio a 1.400 líderes de riesgo y seguridad cibernética del mundo, realizado por la consultora YE se concluye que:

//////

“El 80% de las juntas directivas no hacen de la ciberseguridad un tema estratégico para sus compañías (...). El 87% de las organizaciones todavía operan con niveles limitados de ciberseguridad y resiliencia, mientras que el 77% trabaja con medidas de protección básicas en materia de ciberseguridad y buscan avanzar hacia capacidades más alineadas con la realidad”

//////

¿En qué porcentaje crees que se ubica tu industria? ¿Sientes que tu equipo realmente dimensiona la importancia y transversalidad de la ciberseguridad?

¿La tarea en 2020?: sensibilizarnos frente a la Ciberseguridad

Para **Juan Guillermo Lalinde, coordinador de la maestría en ciencia de los datos y analítica de la Universidad Eafit**, la tendencia de ciberseguridad más importante para este año no será la Inteligencia artificial, el Machine learning o el Big data.

> *“Lo más importante que debe pasar este año es adquirir mayor cultura en ciberseguridad. Que los usuarios de tecnología sean más conscientes sobre el riesgo y las implicaciones que tienen las cosas y la privacidad de sus datos”, declara.*

Y no es ajeno lo que dice Juan Guillermo con lo que recomendaron los especialistas de seguridad de Eset en el video inicial de este especial, y con otros resultados del informe de la consultora EY publicados en el la Revista Dinero.

> *“Entre las principales preocupaciones de las organizaciones están que los empleados inconscientes se clasifican como la mayor debilidad (34%), sumado a que la mayoría de las organizaciones podrían no identificar todas las violaciones e incidentes de las que son víctimas (82%)”.*

Entonces: ¿qué acciones tomar para generar mayor cultura en ciberseguridad?

Volviendo con Juan Guillermo Lalinde, quien además, es coordinador científico del proyecto **Apolo** (iniciativa de investigación y clúster computacional), de la Universidad EAFIT, la respuesta clave está en el autocuidado, la precaución y la educación.

> *“Aún es complicado que los usuarios reconozcan cuándo se enfrentan por ejemplo, a un phishing, a un mensaje de texto fraudulento o a un malware.*
>
> *Lo que se debe hacer es a educar y sensibilizar a los usuarios, para que frente a correos, situaciones sospechosas o extrañas, ni siquiera se detengan a preguntarse si es falsa o verdadera, sino que inmediatamente se comuniquen para validar, ya sea con la entidad bancaria o cualquiera que sea la supuesta empresa destinataria del mensaje”.*

¿Cuáles son los principales riesgos emergentes en esta nueva economía digital?
Descúbrelos en este artículo

AMENAZAS CIBERNÉTICAS A ENTIDADES BANCARIAS

¿SABÍAS QUÉ?

80%

del total de bancos corresponde a código malisioso o *malware.*

63%

del total de bancos corresponde a la violación de políticas de escritorio limpio *(clear desk).*

57%

del total de bancos corresponde a el phishing dirigido para tener acceso a sistemas del banco.

Fuente: Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina.

Y para reforzar la idea de una ciberseguridad con más conciencia para este 2020, hablamos también, con el experto en desarrollo de software y seguridad de la información, Juan David Pineda.

> *“Los ataques se pueden volver más sofisticados, los detalles técnicos pueden cambiar en el tiempo y disfrazarse mucho mejor, entonces, la clave está en la toma de consciencia, porque el usuario no tendrá tiempo de estar actualizado en estos temas por lo rápido que avanzan.*
>
> *Vamos a un caso: existe en la actualidad una USB (Rubber Ducky), que al conectarse a cualquier computadora, instala una puerta trasera y extrae documentos, roba contraseñas sin que la persona se de cuenta. Esta simple USB es en realidad un teclado que digita a velocidades sobrehumanas.*
>
> *Esto lo que significa es que la ciberseguridad va más allá de lo técnico, porque cada vez los ataques se vuelven más sofisticado. Entonces, es necesaria la contramedida de seguridad técnica pero no suficiente y el tema de cultura para enfrentar la ciberseguridad juega un papel fundamental”.*

Buenas prácticas de ciberseguridad para poner en acción

Aquí te dejamos algunas recomendaciones de seguridad informática, entregadas por diferentes expertos, que buscan sensibilizar en ciberseguridad a través de buenas prácticas de autoprotección.

RECOMENDACIONES DE SEGURIDAD INFORMÁTICA

Ningún dispositivo o ninguna persona que esté conectada al ecosistema de la compañía, debe quedar por fuera de las políticas de seguridad de las empresas.

Procura no conectarte a redes inalámbricas que no conozcas.

Si encuentras un dispositivo USB “extraviado” en la calle o un parqueadero, reprime tu curiosidad de saber qué hay en él, aunque no lo creas, puede ser un dispositivo de ataque informático.

Usa fundas de Faraday (están especialmente diseñadas para la preservación y transporte de dispositivos móviles e inalámbricos) para proteger las tarjetas crédito o débito con tecnología pago sin contacto “contactless”. Su uso evita que lleguen señales electromagnéticas “ajenas” y que la información pueda ser leída.

3

6 blogs de ciberseguridad que alimentan tu conocimiento

En ciberseguridad, ataques informáticos, riesgos y amenazas cibernéticas, todo avanza muy rápido.

Por eso, te armamos una lista de blogs recomendados para que no pares de aprender en estos temas, te concientices y generes prevención en tu entorno laboral.

CSIRT Asobancaria

Aunque no es exactamente un blog, este **Ecosistema de colaboración,** conformado por el sector financiero y entidades sin ánimo de lucro, permite anticipar y gestionar de forma efectiva los riesgos del ciberespacio. Ofrece además, actualización constante en alertas de seguridad.

Hacking Ético

Un blog que sobresale por estar enfocado a un público amplio. Tiene posts sobre programación, actualización de aplicaciones, medidas de seguridad, etc. Igualmente genera contenido acerca de cómo proteger dispositivos, alertas de nuevas amenazas y resolver los problemas más comunes de ciberseguridad.

Flu Project

En este sitio encontrarás tutoriales sobre herramientas gratuitas, noticias interesantes, trucos y desafíos, para aprender de hacking responsable aplicado a la seguridad informática.

DragonJar

Este blog ofrece tutoriales para iniciarse en el hacking, seguridad informática defensiva y ofensiva, entrevistas, herramientas y eventos.

MIT Technology Review

Aunque su foco específico no es solo escribir sobre ciberseguridad, el despliegue que hacen sobre tecnologías emergentes, innovación, transformación digital, analítica, entre otros temas, lo hacen un **blog imperdible.**

Reset

No podíamos dejar de auto-recomendarnos. **En nuestro blog** encontrarás artículos enfocados en ciberseguridad y seguridad de la información para la industria financiera. **Y contenidos, podcasts y videos que sabemos pueden ayudarte a fortalecer los conocimientos propios de tu profesión y área laboral.**

4 Reflexiones de Ciberseguridad para 2020

Considerando los temas que serán tendencia en ciberseguridad este año, Cipriano López González, líder de innovación y sostenibilidad de Bancolombia, manifiesta que la cultura de la ciberseguridad comienza por cada uno.

“En la organización se realizan grandes inversiones en la seguridad de cada persona, pero si las personas no tienen autocuidado y autogestión, se estaría vulnerando la seguridad de la organización”.

Cipriano López González

Líder de innovación y sostenibilidad de Bancolombia

“Los colaboradores tenemos una responsabilidad mayor con la seguridad, tenemos que ser más conscientes de qué tipo de información consumo, consulto y comparto; además de las personas con las que me relaciono. En la medida en que cada uno de nosotros cree un anillo de seguridad se multiplica por miles la protección de la organización y así mismo de nuestros cliente externos”.

TOP 5 DE LOS DATOS MÁS VALIOSOS PARA LOS DELINCUENTES CIBERNÉTICOS

17%
Información de los clientes

12%
Información financiera

12%
Planes estratégicos

17%
Información de los miembros de la junta directiva

11%
Contraseñas de los clientes

Tomado de: EY Global Information Security

Así mismo, María Alejandra Lemos, responsable del área de cultura en ciberseguridad de Bancolombia, reflexiona:

> *“Considero que tanto a los empleados, como a los usuarios del sistema financiero a nivel mundial, nos falta mucha conciencia sobre los riesgos de seguridad a los que estamos expuestos, consecuencia del manejo inadecuado que damos a la información financiera confidencial y la forma como usamos los canales y productos digitales. Cada uno tiene responsabilidad sobre la protección de su información, la cual normalmente no asumimos y la descargamos en las entidades.*
>
> *En la industria debemos tener muy presente todos los ecosistemas en los que participamos, ya que somos un eslabón clave para la habilitación de los diferentes servicios y la experiencia del usuario final”.*

¿Todavía sientes el tema de la transformación digital ajeno a tu día a día?
En nuestra **Guía Transformación digital en Colombia** te explicamos porqué no debería continuar así.
¡Anímate a leerla!

PRINCIPALES RIESGOS CIBERNÉTICOS GLOBALES

Ingeniería social

Inyección de código

Garding

Root kids

Cyberbullying

Ataque 0 day

Man in the middle

Sabotaje informático

Spoofing

Jackware

Botnets

Phishing

Man in the browser

Keylogger

Spam

Crimeware

Virus

Malvare

Hijacking

DDos

Adware

Ransomware

Backdoor

Grayware

Suplantación de identidad

Troyano

Riesgos Cirbernéticos

Reset

Una idea **Bancolombia**