UNA HERRAMIENTA PARA PROVEEDORES DE SERVICIOS FINANCIEROS

Desarrollando resiliencia cibernética para la inclusión financiera digital y la innovación

ACCION

MAYO DE 2022

Agradecimientos

Centro Mastercard para el crecimiento inclusivo

En 2018, Mastercard y Acción lanzaron una alianza única en su tipo que une nuestras redes y recursos globales para transformar millones de micro y pequeñas empresas desatendidas, ayudándolas a participar y beneficiarse plenamente de la economía digital. Para resolver este complejo problema, la alianza combina la transformación digital, la innovación fintech, la investigación, el compromiso del sector y la filantropía del talento para brindar herramientas esenciales a las pequeñas empresas, y a los proveedores de servicios financieros que las atienden. A través de nuestra alianza con Mastercard y con el apoyo del Mastercard Impact Fund, trabajamos con nueve proveedores de servicios financieros a nivel mundial para orientar y apoyar sus esfuerzos de desarrollo y adopción de productos y servicios digitales, y así atender de manera más efectiva a un mayor número pequeñas empresas. Estamos muy agradecidos con nuestros socios en Mastercard, incluyendo a su dedicado equipo de liderazgo, personal de programas, voluntariado filantrópico y a los equipos de comunicación, por su apoyo entusiasta a nuestra misión compartida de promover la inclusión financiera y el crecimiento inclusivo.

Acerca del Centro Mastercard para el crecimiento inclusivo

El Centro Mastercard para el Crecimiento Inclusivo promueve a nivel mundial el crecimiento económico equitativo y sostenible, y la inclusión financiera. El Centro aprovecha los activos y competencias medulares de la empresa, incluyendo los conocimientos basados en datos, la experiencia y tecnología, y así mismo; administrando el fondo filantrópico Mastercard Impact Fund para generar investigaciones independientes, aumentar la escala de programas globales y empoderar a una comunidad de pensadores, líderes y actores de vanguardia en cuanto a crecimiento inclusivo. Para obtener más información y recibir sus últimas perspectivas, siga al Centro en Twitter **@CNTR4growth**, **LinkedIn** y **suscríbase** a su boletín.

El autor de este kit de herramientas es Gift Mahubo, director senior en Acción. El autor agradece a todos quienes han contribuido con este kit de herramientas, en particular Emma Morse, Prateek Shrivastava y Charlene Navarra.

Acrónimos y Abreviaturas

API Interfaz de programación de aplicaciones

ATM Cajero automático

HSM Módulo de seguridad en hardware

IA Inteligencia Artificial

IAM Gestión de acceso e identidad

IOT Internet de las cosas

MFA Autenticación multifactor

OTP Contraseña de un solo uso

PAM Gestión de acceso privilegiado

PIN Número de identificación personal

PSF Proveedor de servicios financieros

RD Recuperación de desastres

RPO Punto objetivo de recuperación

RTO Tiempo objetivo de recuperación

SIEM Información de seguridad y gestión de incidentes

Prólogo

Las disrupciones causadas por la pandemia del COVID-19 aceleraron el cambio hacia lo digital, y aumentaron el número de PSF que utilizan tecnologías para agilizar sus operaciones y ofrecer productos y servicios a sus clientes. Se supone que la tecnología apoya a los PSF, pero a menudo se pasa por alto un elemento clave: cada vez más las vulnerabilidades tecnológicas son explotadas y pueden causar perjuicios importantes a los PSF y a los clientes a los que atienden.

Para los clientes de bajos ingresos, la perspectiva de perder incluso pequeñas cantidades de dinero como consecuencia de un ciberataque a su institución financiera puede ser devastadora. Especialmente, como sucede en la mayoría de los países en desarrollo, cuando se produce un incidente cibernético, es el cliente quien sufre las pérdidas y le corresponde además la carga de probar lo contrario. Tales posibilidades disminuyen la confianza de los clientes en las instituciones financieras, y obstaculizan el avance hacia la inclusión financiera.

Más allá de la inclusión financiera, los crecientes riesgos de ciberseguridad amenazan la estabilidad e integridad del sector financiero, así como la protección del consumidor financiero. Los ciberataques también amenazan a los proveedores de servicios financieros digitales con daños reputacionales potencialmente irreparables que podrían conducir a pérdidas de cuota de mercado, y a reducir sus incentivos para innovar.

Por lo tanto, es prudente que los PSF se enfoquen en diseñar, desarrollar e implementar transformaciones digitales para gestionar la seguridad de la información, la privacidad y otros riesgos, a la par que crean tecnologías que ayudan a las personas.

Si los PSF implementan tecnologías para aprovechar oportunidades sin el debido cuidado y sin tener en cuenta los riesgos cibernéticos inherentes, disminuyen las probabilidades de lograr una transformación digital exitosa que cambie la vida de las personas y las proteja. Al enfocarnos en las oportunidades, junto con la obligación de implementarlas de la manera correcta, centrándonos en la ciberseguridad y gestionando los riesgos cibernéticos, podemos lograr que los resultados de la transformación digital y la seguridad digital sean mejores para todos.

En última instancia, no solo los profesionales de la seguridad de la información, sino también los de otras especialidades empresariales, son responsables ante los clientes que atienden, las organizaciones que apoyan, y la sociedad en general, por el logro de una transformación digital segura y beneficiosa.

Prateek Shrivastava
Vicepresidente para lo Digital
Accion Global Advisory Solutions

Kit de herramientas de resiliencia cibernética para proveedores de servicios financieros

La ciberseguridad se refiere a la seguridad de la información y los computadores, pero también tiene en cuenta la protección de la información relacionada y las tecnologías de telecomunicaciones, los datos procesados, la infraestructura, y los productos y servicios que dependen de estas tecnologías. A medida que los PSF se digitalizan, la ciberseguridad se torna fundamental para garantizar que la transformación organizacional resulte "a prueba del futuro", e incluya gobernanza, rendición de cuentas, políticas y procedimientos establecidos adecuadamente, nuevas normas de protección de datos y directrices revisadas y evaluadas de forma constante.

¿Por qué es tan importante la ciberseguridad? El robo de información es el área más rentable y de mayor crecimiento del ciber-crimen. La ciberseguridad protege todas las categorías de datos contra robos y perjuicios, lo que incluye los datos confidenciales, la información de identificación personal, la información personal protegida, la propiedad intelectual y los datos y los sistemas de información del sector. A medida que aumenta el uso de canales digitales por parte de los PSF, también lo hace el riesgo de exponer la información de identidad. El descuidar la ciberseguridad puede impactar a los PSF y causarle muchos costos.

- **Economic**: robo de propiedad intelectual, información corporativa, interrupción del negocio y el costo de reparar sistemas dañados.
- **Reputational**: pérdida de confianza del consumidor, pérdida de clientes actuales y futuros a manos de los competidores y mala cobertura de los medios.
- **Regulatory**: multas o sanciones como resultado de delitos cibernéticos.

El **kit de herramientas de resiliencia cibernética** cibernética para proveedores de servicios financieros contiene lo que Acción ha aprendido ayudando a PSF de todo el mundo a comprender cómo mitigar eficazmente los riesgos cibernéticos y fortalecer la ciberseguridad. Este kit de herramientas está organizado en cinco capítulos principales, cada uno de los cuales contiene orientaciones prácticas para los PSF que implementan planes acción de resiliencia cibernética para proteger mejor sus sistemas, datos y los mejores intereses de sus clientes desatendidos.

Esperamos que esta guía les resulte útil al planificar sus estrategias de ciberseguridad. El objetivo es complementar la **Guía de Transformación Digital de Accion.**

01 Crear apps seguras

Crear aplicaciones móviles con consideraciones de seguridad.

02 Realizar pruebas périodicas para detectar brechas

Entender el proceso de prueba, las capacidades y las medidas correctivas necesarias para proteger a la institución y sus clientes.

03 Crear una cultura de conciencia de ciberseguridad con base en un sólido diseño organizacional

Consejos para construir y mantener una cultura de conciencia cibernética y de manejo de incidentes, producto de la profunda experiencia de Acción en la gestión del cambio.

04 Construir un entorno tecnológico resiliente

Saber cómo crear una infraestructura sólida para proteger y apoyar proactivamente a la institución y a sus clientes antes, durante y después de una amenaza cibernética.

05 Fortalecer la ciberseguridad con las alianzas

Descubrir como entendiendo sus capacidades y el apoyo en alianzas, puede reducir los riesgos cibernéticos y también puede ayudar a gestionar la prestación de servicios a un costo mínimo.

Introducción

La tecnología como motor para superar las barreras a los servicios financieros a gran escala para los desatendidos

La implementación de tecnologías puede ayudar a superar barreras clave que históricamente han llevado a la exclusión de millones de personas del sistema financiero formal. Estos beneficios han traído consigo la creación de nuevas funciones no tradicionales en los proveedores de servicios financieros.

Para beneficiarse de los servicios financieros, las personas deben tener una identidad verificable. El uso de tecnologías como la biometría para la verificación de identidades facilita el proceso de incorporación de nuevos clientes.

Tener una cuenta bancaria no significa inclusión; los clientes solo se benefician cuando hay movimientos de fondos a través de la cuenta. La adopción de nuevas opciones de pago digital facilita este flujo de fondos a la par que proporciona a los clientes un acceso conveniente a sus cuentas.

La inclusión financiera requiere herramientas y recursos que sean útiles en la vida diaria de las personas. Ofrecer a los clientes soluciones para dispositivos móviles y acceso a canales digitales puede aumentar el uso de servicios financieros digitales.

Los productos financieros son complejos. Los clientes no siempre entienden sus beneficios o las opciones que tienen. El uso de la tecnología puede ayudar a los clientes a comprender esta información y a ofrecer productos sencillos y fáciles de usar.

La tecnología ofrece a los proveedores de servicios financieros un potencial ilimitado para impulsar y superar las barreras a la inclusión financiera.

El uso de la tecnología por parte de los proveedores de servicios financieros ha dado lugar a la creación de nuevas funciones no tradicionales:

- **PROTECCIÓN DEL ACCESO DE CLIENTES**
- **PROTECCIÓN DE DATOS**
- **CIBERSEGURIDAD**
- **PROTECCIÓN DE LA IDENTIDAD**
- **DETECCIÓN DE FRAUDES**

La creciente necesidad de que los proveedores de servicios financieros desarrollen nuevas funciones relacionadas con la tecnología pone de manifiesto el aumento de la importancia de desarrollar la resiliencia cibernética para el progreso continuo en la inclusión financiera y la innovación.

¿Por qué ahora la ciberseguridad es importante para los proveedores de servicios financieros?

Se estima que los daños por ciberdelincuencia a nivel mundial alcanzaron los **6 billones de dólares a finales de 2021**, y se espera que crezca un 15% cada año hasta alcanzar los **10,5 billones en 2025** (Cybercrime Magazine, 2020). Esto podría representar la mayor transferencia de riqueza económica de la historia, con ganancias mayores a las del comercio mundial de las principales drogas ilegales juntas.

En la medida en que la complejidad de los sistemas crece exponencialmente, también lo hace la probabilidad de violaciones exitosas a la ciberseguridad. La habilidad de recuperar la infraestructura institucional y las operaciones comerciales en caso de verse comprometidas total o parcialmente puede convertirse en una cuestión de supervivencia para algunas organizaciones.

Muchos factores contribuyen al costo del delito cibernético y pueden atribuirse a enfoques deficientes sobre mejores prácticas de seguridad cibernética. La falta de enfoque en la ciberseguridad puede perjudicar las empresas de los proveedores de servicios financieros de diversas maneras, entre ellas:

COSTOS ECONÓMICOS

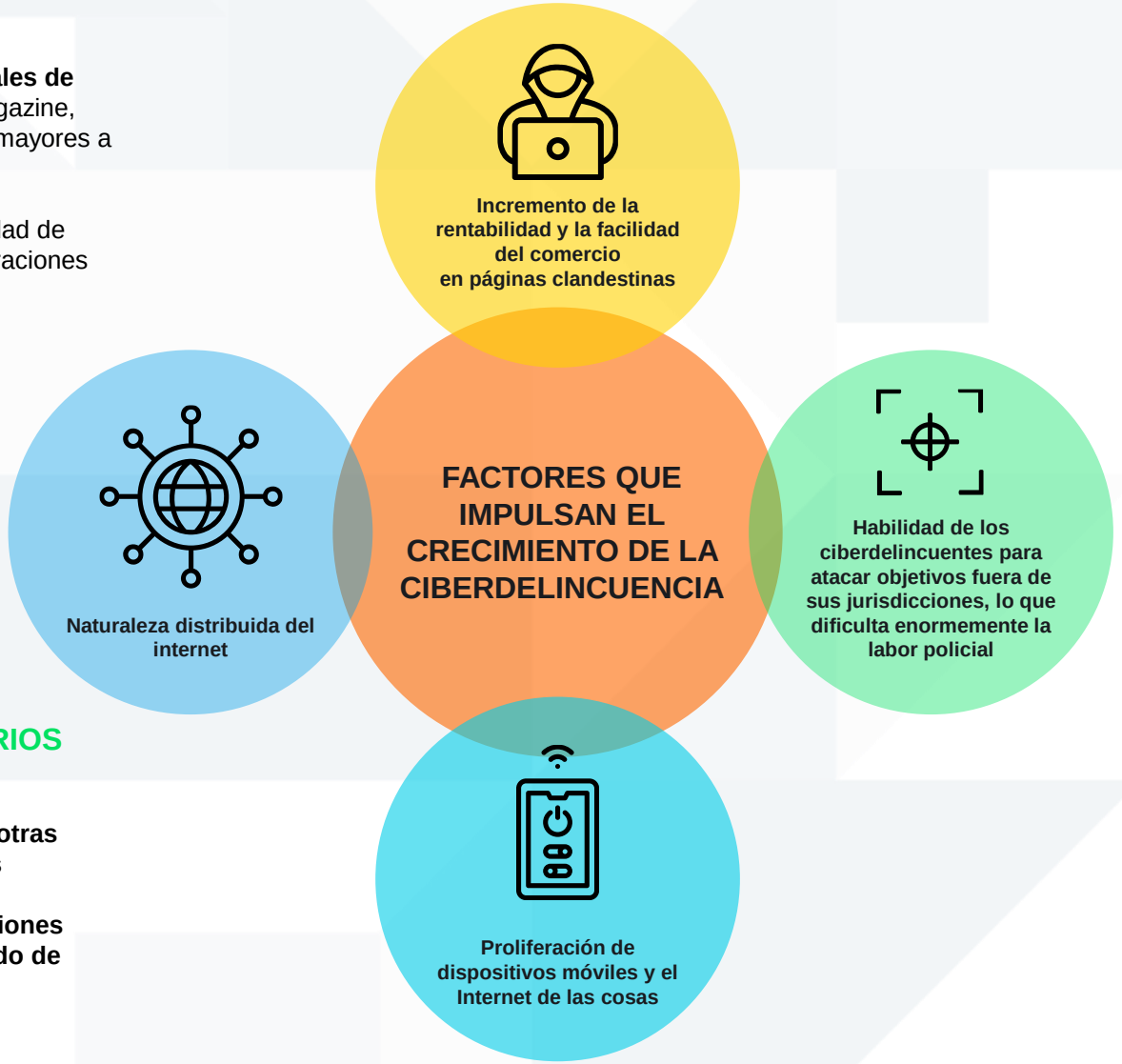
Robo de propiedad intelectual, información corporativa, perturbaciones comerciales y costo de reparación de sistemas dañados

COSTOS REPUTACIONALES

Pérdida de confianza del consumidor, pérdida de clientes actuales y futuros a manos de competidores y mala cobertura de medios

COSTOS REGULATORIOS

La regulación sobre la protección de los datos y otras leyes de exposición de los datos hacen que los PSF incurran en multas o sanciones regulatorias como resultado de delitos cibernéticos.



Cambiando las experiencias de los clientes y tendencias, y el impacto en los PSF

El COVID-19 y los cambios en las experiencias y expectativas de los clientes han llevado a que más PSF desarrollen o adquieran aplicaciones móviles (apps). Las aplicaciones móviles permiten a los PSF mantenerse conectados con los clientes 24/7, mejorando la calidad del servicio y creando un canal importante para cultivar su lealtad.

¿Por qué invertir en el desarrollo de aplicaciones móviles?

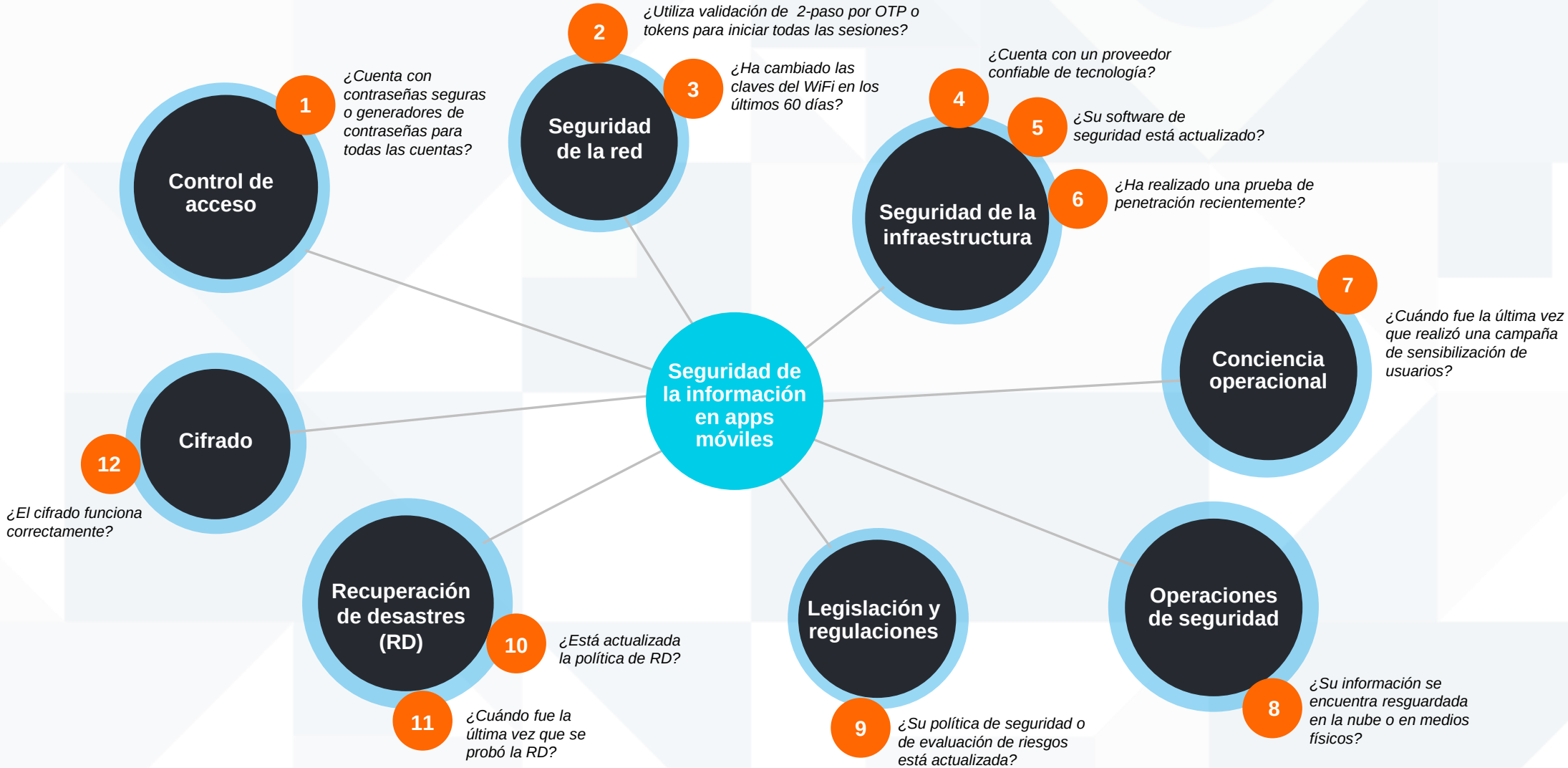
Reduce costos
Las transacciones móviles son mucho más baratas y rápidas que las transacciones en sucursales bancarias y cajeros automáticos tradicionales. Dado que se pueden ejecutar desde cualquier lugar, la necesidad de oficinas físicas disminuye. Los costos operativos y de personal pueden reducirse sin sacrificar el servicio al cliente.

Expansión de la clientela
Los consumidores se sienten atraídos por la conveniencia de las aplicaciones móviles, la accesibilidad en cualquier momento del día y las diversas transacciones realizables a través de billeteras digitales, transferencias, reembolsos, descuentos de compra, vales y cupones aplicables a transacciones futuras. Las aplicaciones móviles pueden ayudar a captar esa primera generación de clientes nativos digitales a medida que se convierten en adultos.

Aumentar la lealtad y la retención del cliente
Las aplicaciones móviles permiten a los clientes conectarse cómodamente 24/7, mejorando así la calidad del servicio y creando un canal importante para cultivar su lealtad. Las notificaciones enviadas pueden informar a los usuarios sobre servicios de crédito, tarifas, nuevas oportunidades y otras actividades. La accesibilidad en cualquier momento del día a su cuenta y transacciones no sólo ayuda a los clientes a sentirse en control, si el servicio es fácil de usar, lo utilizarán más. El soporte profesional proporcionado a través de aplicaciones móviles también mejora la experiencia del cliente, promoviendo una mayor retención del cliente.

Aumentar los ingresos
Las aplicaciones móviles son una forma adicional de comercializar servicios que muchos clientes perciben más favorablemente que las ventas directas en una sucursal. Los PSF con aplicaciones móviles, y especialmente los PSF que solo operan a través de celulares, pueden asociarse con tiendas, cines, restaurantes y otros negocios para ofrecer descuentos a sus clientes dentro de programas mutuamente beneficiosos.

Ensuring mobile app security



Contenido

01 Crear apps seguras
02 Realizar pruebas périodicas para detectar brechas
03 Crear una cultura de conciencia de la ciberseguridad con base en un sólido diseño organizacional
04 Construir un entorno tecnológico resiliente
05 Fortalecer la ciberseguridad con las alianzas

01

Crear apps seguras

Implementando consideraciones de ciberseguridad en el diseño de productos

La incorporación de la seguridad desde las primeras etapas del desarrollo da como resultado **productos y servicios más seguros que pueden ahorrar a las empresas gastos, molestias y la posible desacreditación pública que acompaña las readaptaciones de seguridad.**

MEJORES PRÁCTICAS DE SEGDEVOPS

[1] Pruebas de seguridad de aplicaciones estáticas
[2] Pruebas dinámicas de seguridad de aplicaciones y pruebas interactivas de seguridad de aplicaciones

PLANEACIÓN Y DISEÑO

- Los equipos ágiles tienen conciencia de sus responsabilidades de seguridad desde el principio: hay "campeones de seguridad" en cada equipo
- Los equipos modelan rápidamente las amenazas para todos esfuerzos significativos
- Se crean, priorizan y se hace seguimiento a los elementos del backlog para que cumplan con los requerimientos de seguridad y confiabilidad
- Los diseños de arquitectura segura son preaprobados para implementación

PROGRAMACIÓN

- Los desarrolladores mejoran sus habilidades mediante prácticas seguras y resilientes de codificación
- Se utilizan patrones de codificación, componentes y microservicios reutilizables, para mejorar la seguridad y la agilidad

REVISIÓN

- La seguridad es revisada como parte de cada sprint y liberación de código
- Se utilizan herramientas automatizadas de análisis de codificación (SAST[1]) son usadas para validar la seguridad
- Los desarrolladores senior con experiencia en programación segura, llevan a cabo revisiones entre pares

PRUEBA

- Los miembros de equipos ágiles desarrollan y automatizan casos de prueba de seguridad
- Las pruebas automáticas de penetración (incluyendo DAST e IAST[2]) se llevan a cabo como parte del proceso de desarrollo

DESPLIEGUE

- Los equipos de ingeniería trabajan para mejorar gradualmente la ruta hacía la producción
- Los ambientes de hosting seguros tipo "as code" garantizan eficiencia y repetibilidad
- Se incorporan autenticación y el cifrado robustos

OPERACIÓN

- El monitoreo en tiempo real de las apps garantiza que se detecten problemas de seguridad
- Se implementa la detección de intrusiones a nivel de Host y de redes
- La validación del cumplimiento y la recolección de pruebas es automatizada

https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/agile-reliable-secure-compliant-it-fulfilling-the-promise-of-devsecops

Implementar componentes para aplicaciones móviles seguras

1

PROTEGER LOS DATOS

- Cifrar los datos confidenciales
- Proteger el intercambio de datos

2

PREEVENIR ACCESOS NO AUTORIZADOS

- Construir identidades seguras
- Autenticación a través de PIN, tokens o contraseñas
- Crear niveles apropiados de autorización

3

RECLUTAR LOS RECURSOS ADECUADOS

- Reclutar y utilizar el equipo adecuado de desarrollo de productos
- Utilizar un equipo de implementación motivado
- Crear roles y responsabilidades bien definidos

4

CREAR LA ARQUITECTURA DE SOLUCIÓN ADECUADA

- Proteger el software de la aplicación

5

CREAR Y MANTENER REGISTROS DE SEGURIDAD

- Registrar todo
- Analizar los registros
- Actuar en consecuencia
- Implementar mejoras

6

PROBAR LA SEGURIDAD

- Organizar pruebas basadas en la seguridad
- Realizar pruebas de penetración
- Realizar hacking ético

7

ASEGURAR LOS CANALES DE INTEGRACIÓN

- Comprobar la seguridad de las API
- Utilizar servicios seguros en la nube
- Utilizar tokens seguros para cualquier intercambio de información

8

IMPLEMENTAR UN ESQUEMA DE CERO BRECHAS DE SEGURIDAD

- Integrar la seguridad en los flujos de trabajo diarios

02

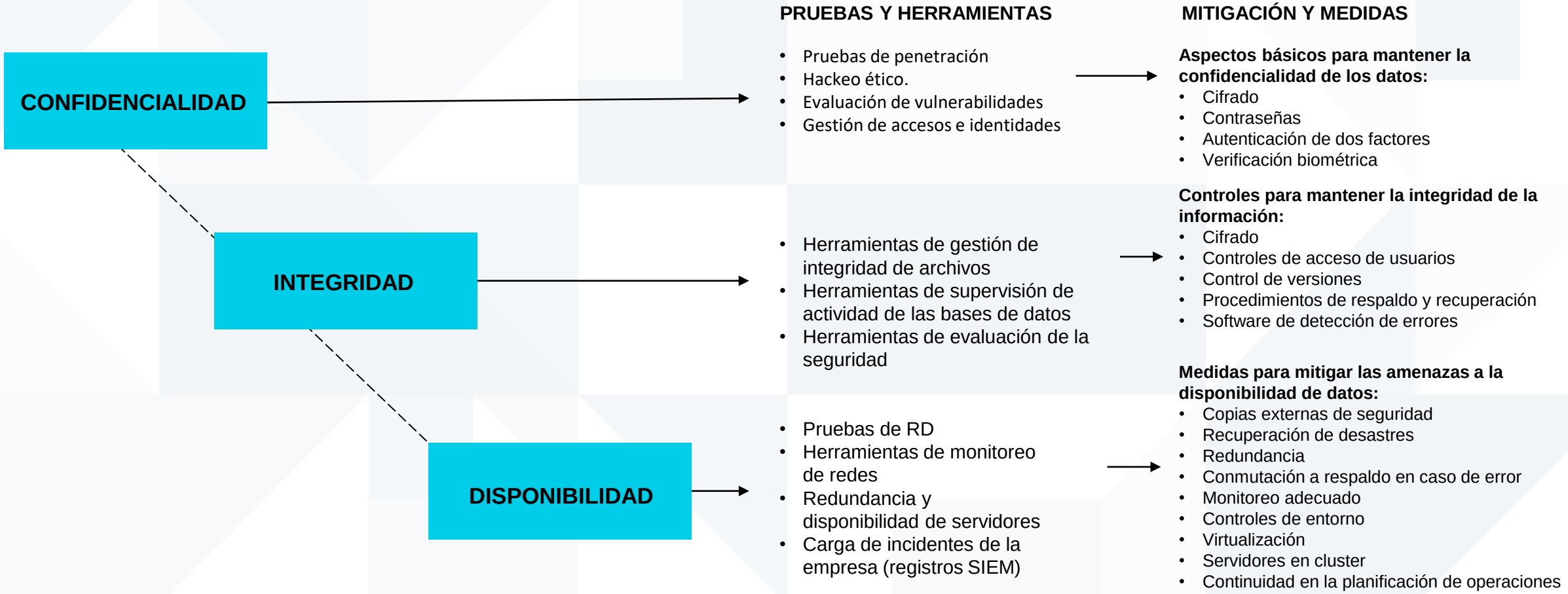
Realizar pruebas périodicas para detectar brechas

Crear una prueba exitosa de proceso y procedimiento

¿Cómo se almacena la información confidencial?	¿*Cómo se mantiene la integridad de los datos?	¿Cómo se definen y aplican los niveles de autenticación?	¿Cómo se mantienen los niveles de acceso?	¿Cuáles son los estándares de disponibilidad mantenidos?	¿Qué tan fácil es repudiar los datos?
Manteniendo un alto nivel de **confidencialidad** de la información ¿Cómo garantizamos que se mantenga la confidencialidad de los datos, enfocada en la protección de la información personal? ¿Qué tan seguro es el intercambio de datos en poder de un cliente con otros usuarios, con terceros?	Midiendo y entendiendo el nivel de **integridad** de los datos ¿Cómo estamos manteni endo la integridad de los datos conservando y garantizando su precisión y exhaustividad durante todo su ciclo de vida? ¿Cómo aseguramos que esos datos no puedan ser modificados de maneras no autorizadas o detectadas?	Comprobando la seguridad de los procesos y pasos de la **autenticación** ¿Cuáles son los procesos y formas existentes de autenticación, y qué hay que mejorar? ¿Cómo verifica el proceso de autenticación que alguien (o algo) es, realmente, quién (o qué) se declara que es? ¿Cuáles son las formas de autenticación en uso? • Características personales (por ejemplo, biométricas) • Algo que usted posee (por ejemplo, OTP o token) • Algo que usted conoce (por ejemplo, PIN o contraseña)	Verificando los niveles de **autorización** y acceso ¿Cuáles son las políticas existentes y los niveles de autorización que otorgan y especifican los derechos/privilegios de acceso a los recursos internos y externos? ¿Se establecen niveles de autorización después de que una persona haya sido identificada y autenticada? ¿Cómo se determina lo que cualquier persona lpueda hacer luego en el sistema?	Configurando y midiendo la **disponibilidad** de la aplicación móvil y de sistemas de soporte ¿Cuáles son los estándares de disponibilidad acordados que certifican que una aplicación móvil está disponible o es accesible por un usuario autorizado, siempre que lo requiera?	Comprobando el nivel de las **soluciones de no repudio existentes** para proporcionar pruebas del origen de los datos y de la integridad de los datos financieros ¿Qué estamos haciendo para garantizar que no haya repudio y que ninguna parte que use la aplicación móvil pueda negar que envió o recibió un mensaje a través del cifrado y/o firmas digitales, o aprobó alguna información? ¿Cómo es posible garantizar que los clientes no puedan negar las transacciones que iniciaron?

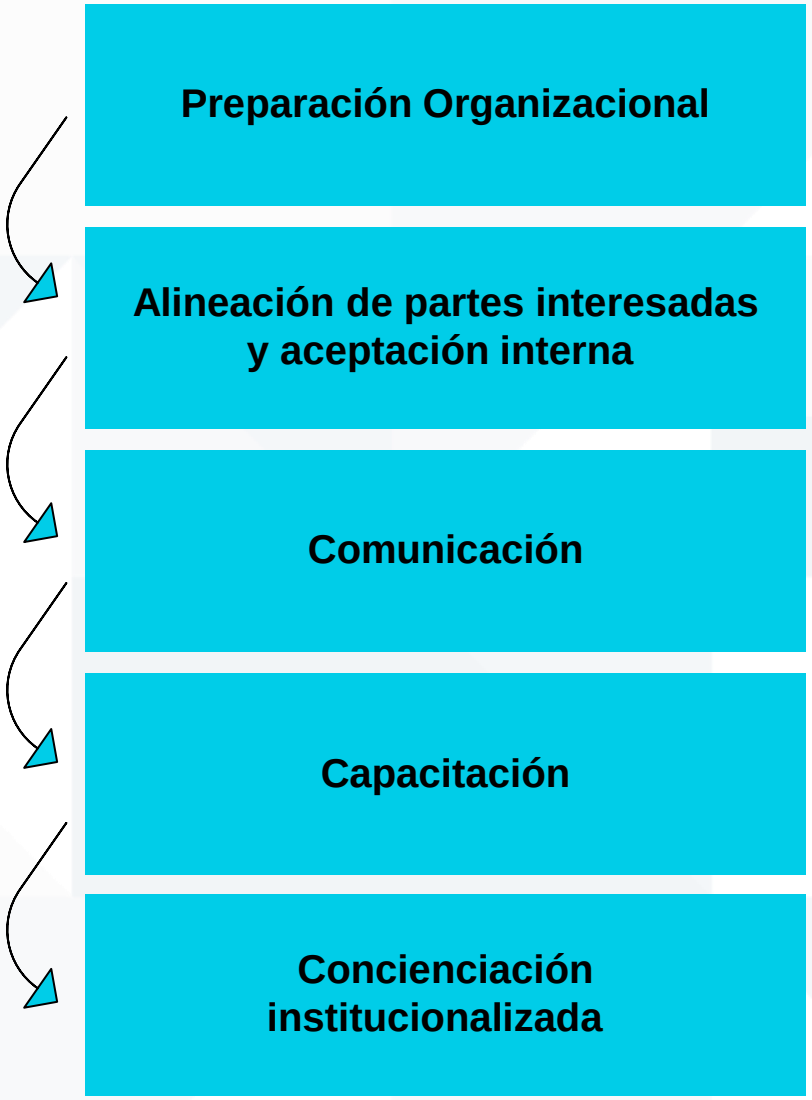
Realizar pruebas regularmente para proteger los datos utilizando el modelo CID *(Confidencialidad, Integridad y Disponibilidad)*

Los PSF de hoy en día se enfrentan a una gran responsabilidad en materia de protección de datos. Ya sea información interna de propiedad exclusiva o cualquier tipo de datos obtenidos de los clientes, podrían enfrentar consecuencias sustanciales en caso de una violación de datos. Es por ello que requerimos contar con los controles de seguridad adecuados para protegernos contra ataques cibertéticos y al mismo tiempo proporcionando seguridad en los documentos y garantizando siempre la disponibilidad de los datos.



03

Crear una cultura de conciencia de ciberseguridad basada en un sólido diseño organizacional



Una cultura de ciberseguridad comienza con la proactividad y la preparación

Un enfoque proactivo puede ayudar a una organización a lograr un mayor grado de preparación para poder reaccionar ante cualquier riesgo o amenaza de ciberseguridad.

La preparación se puede lograr mediante la aceptación y adopción de nuevas:

- Tecnologías
- Procesos
- Comportamientos/Cultura

Consejos para construir una cultura de ciberseguridad

El cambio hacia el trabajo remoto debido al COVID-19 ha creado mayores riesgos de ciberseguridad para las empresas: casi el 60% de los profesionales de seguridad opinaron que trabajar desde casa ha hecho que las organizaciones sean más vulnerables a ataques cibertéticos, y el 60% de las organizaciones han detectado un repunte de moderado a grave en materia de ataques cibernéticos desde el inicio de la pandemia.

Una cultura de ciberseguridad se define como un entorno de trabajo en el que cada persona tiene consciencia de los riesgos cibernéticos y se compromete a reducirlos a través de sus comportamientos y prácticas.

DESAFÍOS A CONSIDERAR

1. Presupuesto
2. La seguridad tiene mala reputación
3. Toxicidad dentro de los equipos cibernéticos
4. El jefe de ciberseguridad o el director de seguridad de la información (CISO) dispone de recursos escasos
5. Los mensajes incoherentes crean confusión

Cerrar la brecha de talentos en ciberseguridad

Uno de los desafíos a los que se enfrentan los PSF ha sido la creciente brecha de talentos en ciberseguridad. La brecha entre la capacidad institucional y lo que requiere la rápida evolución del sector parece ensancharse para la mayoría de los PSF en el mundo, ya que la ciberseguridad es un campo de especialización relativamente reciente con un acelerado cambio en tecnologías y amenazas.

Cerrando la brecha de las habilidades con la automatización (inteligencia artificial)

Una forma de abordar el desafío de la brecha de habilidades es mediante soluciones de automatización de alta tecnología.
Las tecnologías de seguridad impulsadas por inteligencia artificial (IA) ayudan a detectar y a responder rápidamente frente a amenazas sofisticadas.

La automatización de procesos manuales y las alertas de amenazas pueden ayudar a llenar vacíos críticos. Sin embargo, también hay que considerar los recursos y equipos existentes para abordar este tema de manera integral.

Nuevas fuentes de talento, nuevas oportunidades

Un resultado positivo de la pandemia son las numerosas oportunidades profesionales en el campo de la ciberseguridad.

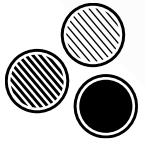
A medida que el concepto de trabajo remoto se convierte en la norma, y las infraestructuras se tornan cada vez más distribuidas, la necesidad de profesionales en TI que tengan habilidades y conocimientos sobre seguridad estará en aumento.

La necesidad de roles como científicos de datos, personal de cumplimiento normativo con conocimientos cibernéticos o los cazadores de amenazas sólo se espera que incremente.

Superar el aumento de riesgos

Con la pandemia creando un turno de trabajo remoto masivo y el consiguiente aumento de riesgos cibernéticos, encontrar personas con habilidades en ciberseguridad resulta más difícil que nunca.

Empleadores y empleados pueden ayudar a superar este desafío a través de cursos y certificaciones, brindando así mayor seguridad organizacional en medio de tiempos difíciles.



Aumentar la diversidad al ofrecer igualdad de oportunidades

Las organizaciones están cambiando el proceso de reclutamiento y las fuentes de contratación para aprovechar esta posible veta.

El alentar de manera proactiva el desarrollo de una fuente de talentos diversa e inclusiva requiere que los líderes comprendan los problemas complejos alrededor del tema y demanden su aceleracion.

Evaluar la madurez de la cultura de ciberseguridad

	→ ETAPA 1: INCIPIENTE	→ ETAPA 2: EN DESARROLLO	→ ETAPA 3: AVANZADA
ACTITUDES **Sentimientos y creencias de los empleados sobre los protocolos y problemas de seguridad.**	Los empleados creen que los protocolos de seguridad deben ser manejados por TI	Los empleados creen que tienen un papel en la mitigación de las amenazas de seguridad, pero piensan que la mayoría de los problemas serán gestionados por TI	Los empleados entienden la importancia de los protocolos de seguridad y perciben su papel en su cumplimiento
COMPORTAMIENTOS **Acciones de los empleados que afectan la seguridad, directa o indirectamente**	Los empleados no se ciñen a las precauciones básicas de seguridad	Los empleados observan algunas precauciones de seguridad, pero no toman medidas activas de mitigación	Los empleados toman medidas para mitigar activamente las posibles amenazas a la seguridad
COGNICIÓN **Comprensión, conocimientos y conciencia de los empleados sobre los problemas y actividades a llevar a cabo alrededor de la seguridad**	Los empleados tienen una conciencia limitada de los posibles problemas de seguridad y de lo que pueden hacer para mitigarlos	Los empleados tienen cierta conciencia de posibles problemas de seguridad	Los empleados están bien informados de los problemas de seguridad
COMUNICACIÓN **Qué tan bien promueven los canales de comunicación un sentido de pertenencia y ofrecen apoyo relacionado con problemas de seguridad y reportes de incidentes.**	La comunicación sobre amenazas de seguridad solo se genera cuando se ha producido un incidente	Tecnología envía ocasionalmente comunicaciones al personal sobre la prevención de amenazas a la seguridad	Los empleados de toda la organización se comunican de forma regular y proactiva sobre problemas de seguridad y su mitigación
CUMPLIMIENTO **Conocimientos de los empleados y apoyo a las políticas de seguridad**	Los empleados no cumplen con las políticas básicas de seguridad	Los empleados cumplen con la mayoría de las políticas de seguridad	Los empleados cumplen con las políticas de seguridad casi universalmente
NORMAS **Conocimientos del empleado y cumplimiento de normas de conducta no escritas relacionadas con la seguridad.**	Las normas organizacionales en materia de conciencia de seguridad son inexistentes y/o los empleados las entienden poco	Puede que las normas de seguridad existan a nivel organizacional, pero no son cumplidas por todos	Las normas de seguridad están bien documentadas, comprendidas y observadas por la mayoría del personal
RESPONSABILIDADES **Cómo perciben los empleados su papel como factor crítico para ayudar o perjudicar la seguridad.**	La mayoría de los empleados no creen que desempeñan un papel activo en la prevención de brechas de seguridad	Algunos empleados creen que desempeñan un papel activo en la prevención de fallas de seguridad	Todos los empleados creen que desempeñan un papel activo en la prevención de fallas de seguridad

https://www.forbes.com/sites/forbesbusinesscouncil/2021/05/27/the-importance-of-a-strong-security-culture-and-how-to-build-one/?sh=4e0fa8476d49

Evite las trampas comunes

NO ESPERE A QUE OCURRA UN INCIDENTE.

Si se espera a que ocurra un ataque cibernético, ya es demasiado tarde para actuar. Sea proactivo en la implementación de una cultura consciente del riesgo cibernético. Los cambios culturales pueden tardar un tiempo en que sucedan, por lo que es importante comenzar pronto y monitorear los progresos con frecuencia.

ALINEE LOS OBJETIVOS DE LA CULTURA CON LA ESTRATEGIA DE GESTIÓN DE RIESGOS CIBERNÉTICOS.

Los objetivos de cambio de cultura deben estar alineados con la estrategia general de gestión de riesgos cibernéticos de la organización. Asegúrese que los objetivos de cambio cultural incluyan la mitigación de los riesgos cibernéticos usuales, incluyendo los impactos operativos o de denegación de servicio.

ADAPTE LOS ESFUERZOS A SUS EMPLEADOS.

No existe una solución única para todos cuando se trata de una cultura de ciberseguridad. Segmente al personal y personalice su participación, comunicación y capacitación, y evaluación en función de estos atributos.

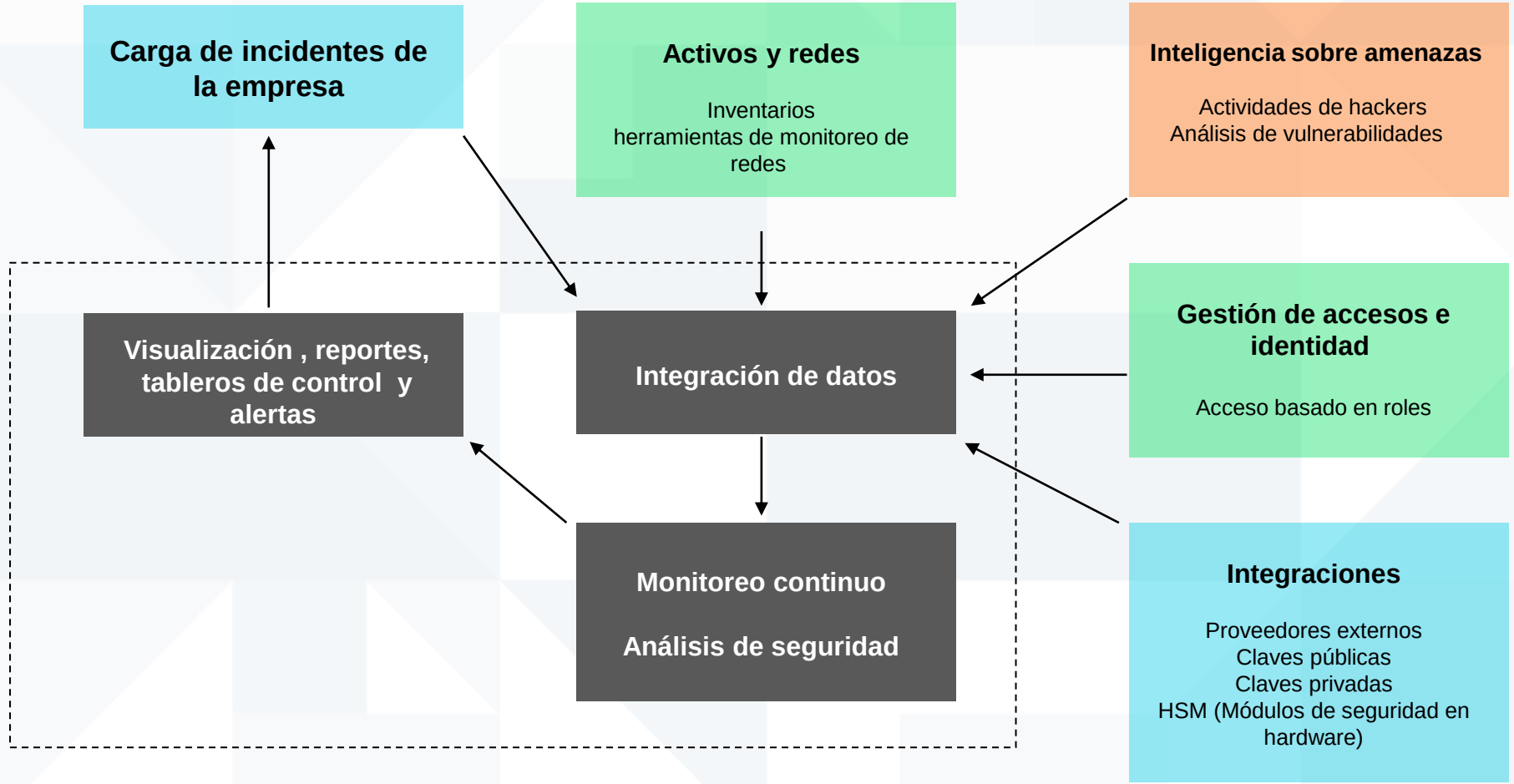
ADOPTE UN ENFOQUE OMNICANAL PARA LOS MENSAJES.

Para ser efectiva, una campaña de cultura de riesgo cibernético debe aprovechar múltiples canales de comunicación. Estudie cómo sus empleados aprovechan los canales de comunicación actualmente, y piense en formas de llevarles contenido de manera creativa y efectiva. Aproveche principios conductuales como los recordatorios y el efecto de ”comenzar desde cero" para programar los mensajes para que tenga el máximo impacto.

PRUEBE Y EXPERIMENTE.

Entender lo que funciona mejor probando iniciativas con grupos más pequeños antes de implementar estrategias con toda la organización. Pruebe contenidos, el mejor momento de enviarlos, su tamaño y los canales para comprender qué funciona mejor cuando se trata de implementar nuevas prácticas.

Diseño de una arquitectura de seguridad de alto nivel



Implementando las etapas para un plan de recuperación

IDENTIFIQUE EL ALCANCE DE SU PLAN DE RECUPERACIÓN ANTE DESASTRES

El plan de recuperación ante desastres identifica de forma exacta qué se planea recuperar, dónde se respaldará la información, las políticas comerciales subyacentes y el impacto comercial sobre estas decisiones.

PROPORCIONE UNA VISIÓN GENERAL DE LAS OPERACIONES, LA GOBERNANZA Y LA RENDICIÓN DE CUENTAS

Proporcione una visión general sobre las operaciones, la gobernanza y la rendición de cuentas, los tomadores de decisiones e identificar quién es responsable de cada parte del plan de recuperación de desastres.

IDENTIFIQUE LOS SISTEMAS CLAVE A SER RECUPERADOS

Identifique los sistemas clave que deben recuperarse en caso de desastre. Documente los perfiles de aplicaciones, los sistemas prioritarios y los perfiles del sistema. Tenga en cuenta:

- Punto de Recuperación Objetivo (PRO): la antigüedad de los datos que se desean restaurar.
- Tiempo Objetivo de Recuperación(TOR): el tiempo necesario para recuperarse ante un desastre.

PROPORCIONE UN INVENTARIO

Proporcione un inventario de los elementos que deberán restaurarse en caso de desastre.

IDENTIFIQUE LOS PROCEDIMIENTOS DE NOTIFICACIÓN Y ACTIVACIÓN

Describa las acciones que se deben tomar para detectar y evaluar los daños causados por una interrupción del sistema. Con base en la evaluación del incidente, el gerente de recuperación activará el plan.

DESCRIBA LOS PROCEDIMIENTOS PARA RECUPERAR EL SISTEMA EN EL SITIO DE RESPALDO

Documente los procedimientos para recuperar el sistema en el sitio alterno. Realice cada procedimiento en la secuencia prevista para mantener operaciones eficientes.

PRUEBE EL PLAN DE RECUPERACIÓN

Asegurese de que el plan sea probado y mantenido para que siga siendo relevante y confiable si ocurre un desastre. El propietario del documento es responsable de garantizar que el plan refleje con precisión los pasos de recuperación, los detalles de contacto y las referencias que pueden cambiar con el tiempo.

IDENTIFIQUE LOS RECURSOS DE LOS SITIOS ALTERNOS

Destaque los recursos requeridos en el sito alternativo (es decir, el sitio al que se mudará después de un desastre) para garantizar que las operaciones se puedan realizar correctamente.

IDENTIFIQUE LAS ACTIVIDADES PARA RESTAURAR OPERACIONES EN EL SITIO ORIGINAL, O EN EL NUEVO

Cuando el sitio original ha sido restablecido, se deben regresar las operaciones desde el sitio alterno. La meta es proporcionar una transición fluida de las operaciones desde el sitio alternativo al sitio original.

DESCRIBA EL PROCESO DE COMUNICACIÓN

Describa el proceso de comunicación en caso de una situación de desastre. Se requiere comunicación externa para mantener informadas a las partes interesadas clave sobre la situación, los problemas y los riesgos del proyecto.

Enfoque del plan de recuperación

Continuidad del negocio describe cómo un negocio procederá durante y después desastre. Este provee planes de contingencia, descubriendo cómo continuará operando el negocio si tiene que mudarse a una ubicación alterna. La planificación de la continuidad del negocio también puede considerar interrupciones más pequeñas o desastres menores, como cortes de energía prolongados.

Recuperación de desastres se refiere a los planes que una empresa pone en marcha para responder a un evento catastrófico, tal y como un desastre natural, fuego, actos terroristas o crimen cibernético La recuperación de desastres implica las medidas que toma una empresa para responder a un evento y regrese a la operación normal y segura lo más rápido posible.

La continuidad del negocio se enfoca en mantener el negocio operativo durante un desastre, mientras que la recuperación ante desastres se enfoca en restaurar el acceso a los datos y la infraestructura de tecnología después de un desastre.

Los planes efectivos de continuidad comercial limitan el tiempo de inactividad operativo, mientras que los planes efectivos de recuperación ante desastres limitan las funciones anormales o ineficientes del sistema.

Plan de continuidad de negocio

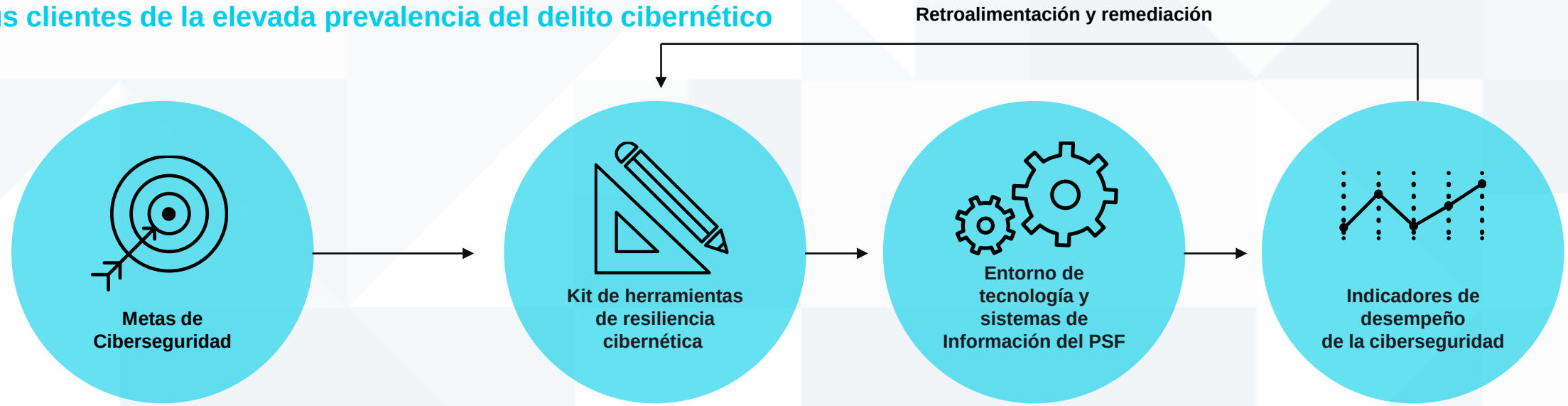
Plan de recuperación

04

Construir un entorno tecnológico resiliente

Implementar una estrategia de ciberresiliencia

El desarrollo e implementación de una estrategia de ciberresiliencia es esencial para proteger a la institución y a sus clientes de la elevada prevalencia del delito cibernético



- Proteger la confidencialidad de los datos
- Preservar la integridad de los datos
- Promover la disponibilidad de los datos para usos autorizados

1. Impacto sobre clientes
2. Grandes aumentos (o disminuciones) de incidentes reportados
3. Número total de incidentes de seguridad
4. Costos por incidente
   - Costos directos
   - Costos indirectos
   - Costos de oportunidad
5. Tiempo de actividad
6. Estándares normativos
7. Tiempo para resolver

Adoptar un plan de acción de ciberseguridad

Crear un plan de acción de ciberseguridad exitoso utilizando los cinco pilares críticos

Identificar

- Gestión de activos
- Entorno del negocio
- Gobernanza
- Evaluación de riesgos

Proteger

- Control de activos
- Cursos de Concientización
- Seguridad de los datos
- Protección de la Información
- Procesos y procedimientos
- Tecnología de protección

Detectar

- Anomalías e incidentes
- Monitoreo continuo de seguridad
- Procesos de detección
- Pruebas de penetración
- Hackeo ético.

Responder

- Planificación de recursos
- Comunicaciones
- Análisis
- Mitigación
- Mejoras

Recuperar

- Planificación de la recuperación
- Mejoras
- Pruebas
- Comunicación
- Documentación

Maximizar la protección, minimizar los riesgos.
Concentrarse en implementar los elementos clavede un enfoque de seguridad moderno para maximizar la protección y minimizar los riesgos.

Identifique las amenazas cibernéticas y proteja sus datos

Las medidas de ciberseguridad protegen sus datos y le ayudan a mantener la ventaja competitiva. Los agentes de amenazas cibernéticas pueden llevar a cabo ataques para interrumpir sus actividades, robar datos para venderlos o dar ventajas a los competidores. Es importante proteger los datos.

AMENAZAS CIBERNÉTICAS USUALES

Phishing
Llamadas, mensajes de texto, correos electrónicos o uso de redes sociales para llevarlo a que haga clic en un enlace malicioso, descargar malware, un software malicioso o compartir información confidencial.

Amenazas internas
Cualquier persona que tenga acceso a la infraestructura y los datos de una organización puede causar daño intencional o involuntario.

ENFOQUES PARA PROTEGER LOS DATOS

CAPACITAR A QUIENES TENGAN ACCESO A LA INFORMACIÓN INSTITUCIONAL
Capacitar a todo el personal, contratistas y otras personas con acceso a información institucional para ayudarlos a entender sus roles en la protección de la institución contra las amenazas cibernéticas.

UTILIZAR LA AUTENTICACIÓN MULTIFACTOR
La autenticación multifactor utiliza dos o más métodos diferentes para verificar las identidades (factores de autenticación).

INSTALAR SOFTWARE Y HERRAMIENTAS DE SEGURIDAD
Instalar herramientas de seguridad en sistemas y dispositivos, como firewalls y software antivirus, que ayuden a proteger los sistemas y redes institucionales del malware.

ACTUALIZAR Y "PARCHEAR" DISPOSITIVOS Y SOFTWARE
Actualizar y aplicar parches/actualizaciones con frecuencia a los dispositivos y el software para proteger los sistemas de las vulnerabilidades de seguridad y reducir los riesgos de las amenazas cibernéticas.

IMPLEMENTAR CONTROLES DE ACCESO
Asegurarse que el personal, los contratistas y otras personas con acceso a la información institucional solo tengan los privilegios necesarios para su trabajo específico. Utilizar credenciales individuales de inicio de sesión y revocar el acceso cuando ya no sea necesario.

REALIZAR COPIAS DE SEGURIDAD DE DATOS
Respaldar los datos institucionales en un dispositivo que no esté conectado directamente a su red principal para proteger las copias de seguridad de posibles ciberataques en los sistemas primarios (por ejemplo, ransomware) y permitir una ruta para restaurar de ser necesario. Probar las copias de seguridad con regularidad.

Mantener una evaluación continua de un marco equilibrado

Un marco bien diseñado y equilibrado en cuanto a riesgos se basa en:

Excelencia operacional
Capacidad de ejecutar y monitorear sistemas para proporcionar valor comercial a la par de mejorar continuamente los procesos y procedimientos de soporte.

Seguridad
Capacidad para proteger la información, los sistemas y los activos sin dejar de ofrecer valor comercial a través de evaluaciones de riesgos y estrategias de mitigación.

Confiabilidad
Capacidad para garantizar que los sistemas puedan recuperarse de disrupciones de infraestructura o servicios, adquirir dinámicamente recursos informáticos para satisfacer la demanda y mitigar perturbaciones como configuraciones erróneas o problemas transitorios de redes.

Eficiencia del desempeño
Capacidad de utilizar los recursos de manera eficiente para cumplir con los requisitos del sistema y mantener el rendimiento a medida que la demanda cambia y las tecnologías evolucionan.

Optimización de costos
capacidad para ejecutar sistemas que proporcionan valor comercial al precio más bajo minimizando o evitando costos innecesarios.

05

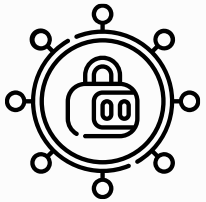
Fortalecer la ciberseguridad con las alianzas

¿Por qué las asociaciones exitosas son fundamentales para promover la ciberseguridad?

Las asociaciones estratégicas pueden ser una estrategia eficaz para aumentar la seguridad de los sistemas y mitigar el riesgo de ataques cibernéticos.

BENEFICIOS CLAVE DE LAS ASOCIACIONES DE CIBERSEGURIDAD

- Abordar las brechas de destrezas en ciberseguridad
- Obtener acceso a expertos en ciberseguridad según se requiera
- Fácil acceso a la información
- Liberar tiempo y recursos de personal



BARRERAS PARA UNA COLABORACIÓN EFECTIVA

- Confianza y control en respuesta a incidentes
- Preguntas en torno a las obligaciones de divulgación y exposición
- Evolución de la responsabilidad y el panorama regulatorio
- Desafíos a los que se enfrenta la investigación transfronteriza de delitos cibernéticos
- Restricciones transfronterizas de transferencia de datos que impiden a las empresas responder a ciberamenazas e incidentes

10 formas de evaluar asociaciones de ciberseguridad

1. ¿La solución del socio es una integración adicional o integrada?
2. ¿La hoja de ruta del producto está sincronizada con los lanzamientos gustdel proveedor principal?
3. Cuidarse de soluciones de socios que requieren nuevas plataformas IAM o PAM.
4. ¿Es eficiente la asociación en la generación de código a nivel de producción cuando se crece?
5. ¿El socio adicional va a ayudar o a perjudicar al negocio?
6. Entrevistar a los clientes referidos que ejecutan la solución del socio.
7. ¿Cuál es el historial compartido de incidentes de la asociación?
8. La indemnización de terceros es imprescindible.
9. Incluir auditorías de seguridad externas y aleatorias en el contrato.
10. ¿Qué tan seguros son los ciclos de DevOps que los socios comparten para crear productos?

Gracias.

ACCION