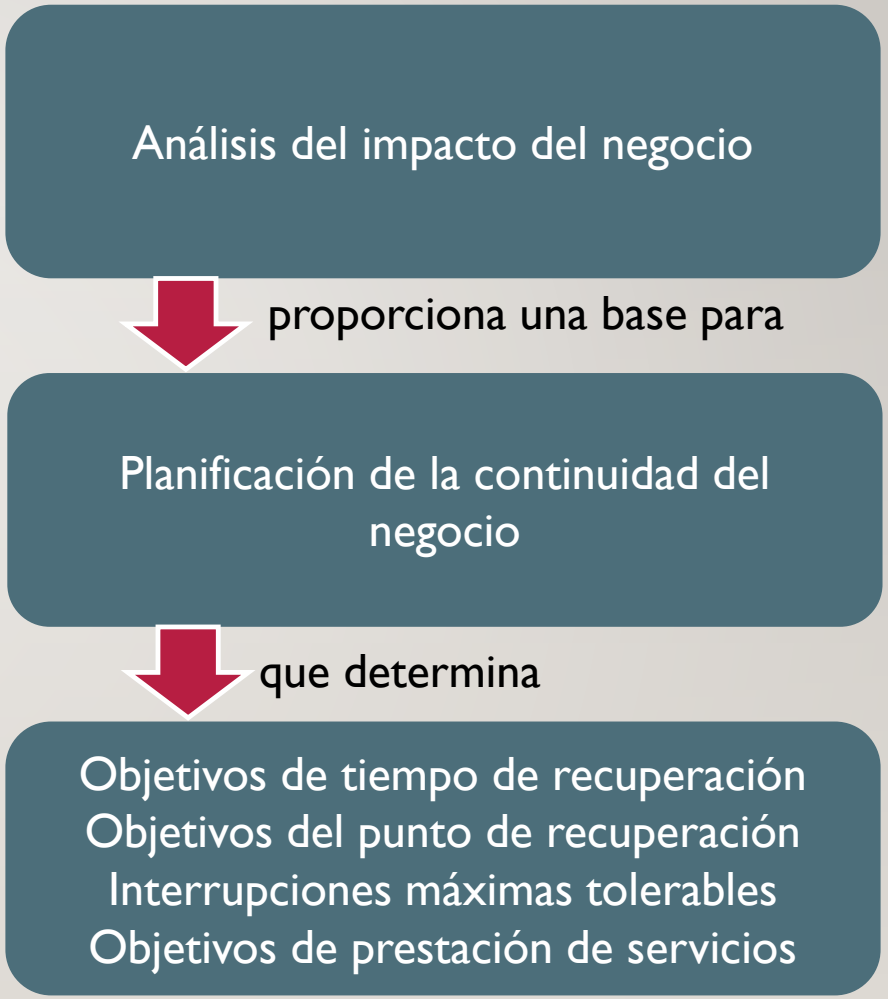
PLANIFICACIÓN DE LA CONTINUIDAD DEL NEGOCIO

En resumen, el sistema de información BCP / DRP es un componente importante de la estrategia general de continuidad del negocio y recuperación ante desastres de una organización.

El proceso de BCP está respaldado por un análisis considerado de los impactos comerciales.



RECUPERACIÓN

La recuperación de datos es el proceso de restaurar los datos que se han perdido, eliminado accidentalmente, dañado o inaccesible por cualquier motivo.

Los procesos de recuperación varían según el tipo y la cantidad de datos perdidos, el método de respaldo empleado y los medios de respaldo.

APOYO

Los procedimientos de copia de seguridad se utilizan para copiar archivos a un segundo medio, como un disco, una cinta o la nube.

Los archivos de respaldo deben mantenerse en una ubicación externa.

Existen tres tipos de copias de seguridad de datos: completa, incremental y diferencial.

Completo	Incremental	Diferencial
• Copia todos los archivos seleccionados en el sistema por completo, independientemente del estado reciente de la copia de seguridad. • Método de copia de seguridad más lento, pero más rápido para restaurar datos.	• Copia todos los archivos que han cambiado desde que se realizó la última copia de seguridad, independientemente de si la última fue una copia de seguridad completa o incremental. • Método de copia de seguridad más rápido, pero más lento para restaurar datos.	• Copia solo los archivos que han cambiado desde la última copia de seguridad completa. • El archivo crece hasta que se realiza la siguiente copia de seguridad completa.

SECCIÓN 6

Implicaciones de seguridad y adopción de tecnología en evolución

TEMAS CUBIERTOS EN ESTA SECCIÓN

1. Tendencias en el panorama actual de amenazas.
2. Características y objetivos de las amenazas persistentes avanzadas (APT).
3. Vulnerabilidades, amenazas y riesgos de dispositivos móviles.
4. La consumerización de TI y dispositivos móviles.
5. Riesgos y beneficios de la colaboración en la nube y digital.

TEMA 1:

Paisaje actual de amenazas

RIESGO DE CIBERSEGURIDAD

La creciente dependencia de las tecnologías digitales hace que las organizaciones sean más susceptibles al riesgo de ciberseguridad.

PANORAMA DE AMENAZAS

Un panorama de amenazas, también conocido como entorno de amenazas, es una colección de amenazas. El panorama de amenazas de ciberseguridad está cambiando constantemente. Las tendencias recientes en el panorama de amenazas cibernéticas incluyen:

- Los agentes de amenazas son más sofisticados en sus ataques y uso de herramientas.
- Los patrones de ataque se están aplicando a dispositivos móviles.
- Los estados nacionales tienen la capacidad de infiltrarse en objetivos gubernamentales y privados (guerra cibernética).
- La computación en la nube da como resultado grandes concentraciones de datos dentro de un pequeño número de instalaciones, creando objetivos atractivos para los atacantes.
- Las redes sociales se han convertido en un canal principal para la comunicación, la recopilación de conocimientos, el marketing y la difusión de información.
- La popularidad de Big Data como un activo permite el potencial de infracciones a gran escala.

TENDENCIAS RECIENTES EN CIBERSEGURIDAD

La información de ENISA (2015) muestra las siguientes tendencias en el panorama de amenazas:

Creciente	Estable	Declinante
• Malware • Ataques basados en la web • Ataques a aplicaciones web • Negación de servicio • Amenazas internas (maliciosas o accidentales) • Kits de explotación • Fuga de información • Secuestro de datos • Espionaje cibernético	• Daño físico / robo / pérdida • Suplantación de identidad • Violaciones de datos • El robo de identidad	• Botnets • Correo no deseado

TEMA 2:

Amenazas persistentes avanzadas

¿QUÉ ES UNA AMENAZA PERSISTENTE AVANZADA?

Una amenaza persistente avanzada (APT) es una amenaza dirigida que se compone de varios vectores de ataque complejos y puede permanecer sin detectar durante un período prolongado de tiempo.

A diferencia de muchos otros tipos de actos criminales, no se desvía fácilmente por una respuesta defensiva determinada.

Además, los APT tienen las siguientes características:

- Grado de planificación sin precedentes, recursos empleados y técnicas utilizadas.
- A menudo siguen un modus operandi particular.

OBJETIVOS APT

Los APT se dirigen a empresas de todos los tamaños en todos los sectores de la industria y todas las regiones geográficas que contienen activos de alto valor.

Ninguna industria con secretos valiosos u otras fuentes de ventaja comercial que puedan ser copiadas o socavadas a través del espionaje está a salvo de un ataque APT.

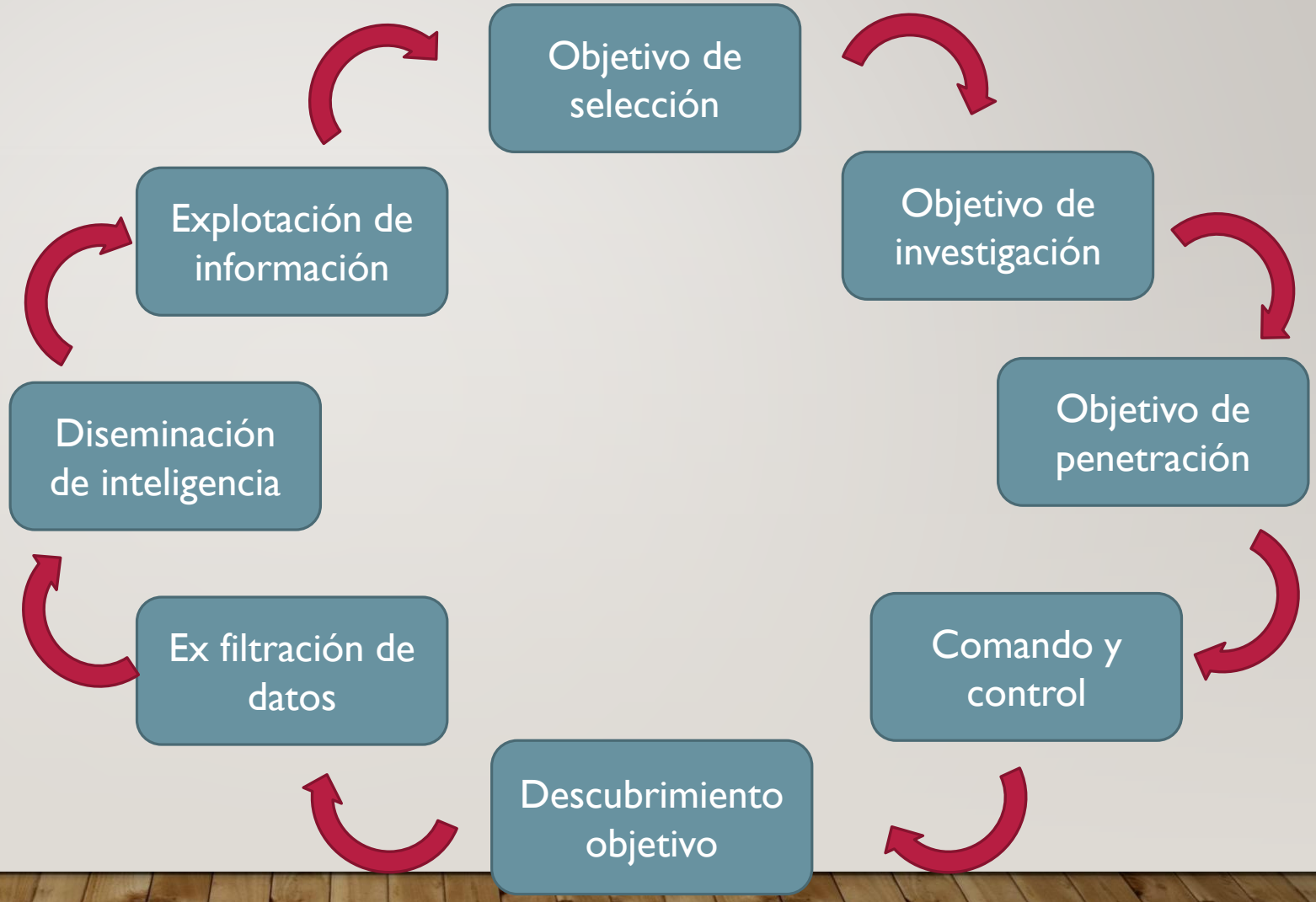
Los ataques APT a menudo abarcan organizaciones de terceros que prestan servicios a empresas específicas.

APT FUENTES DE AMENAZA

AMENAZA	LO QUE BUSCAN	IMPACTO DE NEGOCIOS
Agencias de inteligencia	Secretos comerciales políticos, de defensa o comerciales.	Pérdida de secretos comerciales o ventajas comerciales competitivas.
Grupos criminales	Transferencias de dinero, oportunidades de extorsión, información de identificación personal o secretos para una posible venta posterior.	Pérdida financiera, violación de datos de clientes a gran escala o pérdida de secretos comerciales.
Grupos terroristas	Producción de terror generalizado a través de la muerte, destrucción e interrupción.	Pérdida de producción y servicios, irregularidades del mercado de valores y riesgo potencial para la vida humana.
Grupos activistas	Información confidencial o interrupción de los servicios.	Gran violación de datos o pérdida de servicios
Fuerzas armadas	Inteligencia o posicionamiento para soportar futuros ataques a infraestructura nacional crítica.	Daños graves a las instalaciones en caso de conflicto militar.

ETAPAS DE UN ATAQUE APT

Aunque no hay dos ataques APT exactamente iguales, a menudo siguen un ciclo de vida similar que comienza con la selección de objetivos y la investigación.



TEMA 3:

Tecnología móvil: vulnerabilidades, amenazas y riesgos.

SEGURIDAD PARA TECNOLOGÍA MÓVIL

La seguridad para la tecnología móvil es una función del riesgo asociado con su uso.
Las amenazas relacionadas con la tecnología móvil incluyen las que se enumeran aquí.

1. Uso inadecuado de la plataforma.
2. Almacenamiento inseguro de datos.
3. Comunicación insegura.
4. Autenticación insegura.
5. Criptografía insuficiente.
6. Autorización insegura.
7. Calidad del código del cliente.
8. Manipulación de código.
9. Ingeniería inversa.
10. Funcionalidad extraña

RIESGO TÉCNICO

Los dispositivos móviles presentan una serie de riesgos técnicos, además de riesgos físicos y organizativos.

- Monitoreo de actividad y recuperación de datos
- Conectividad de red no autorizada
- Vista web / interfaz de usuario
- Fuga de datos confidenciales
- Almacenamiento de datos
- Transmisión de datos confidenciales inseguras
- Vulnerabilidades de manejo

CONTROL DE ACTIVIDAD Y RIESGO DE RECUPERACIÓN DE DATOS

OBJETIVO	RIESGO
Mensajeria	Ataques genéricos a texto SMS, transmisión de texto y contenido enriquecida con MMS. Recuperación de contenidos de correo electrónico en línea y fuera de línea. Inserción de comandos de servicio por textos de difusión celular SMS. Ejecución de código arbitrario a través de SMS / MMS. Re direccionar o ataques de phishing por texto SMS o correo electrónico habilitados para HTML.
Audio	Inicio de llamadas encubiertas o grabación de llamadas. Grabación de micrófono abierto.
Imagenes/Video	Recuperación de imágenes y videos al aprovechar la funcionalidad habitual de "compartir" en la mayoría de las aplicaciones. Captura encubierta de video o imágenes, incluida la limpieza sin trazas de dicho material.
Geolocalizacion	Monitoreo y recuperación de datos de posicionamiento GPS, incluidas marcas de fecha y hora.
Dato estadistico	Intelligence or positioning to support future attacks on critical national infrastructure.
Historia	Monitoreo y recuperación de todos los archivos de historial en el dispositivo o en tarjetas SIM (llamadas, SMS, navegación, entrada, contraseñas almacenadas, etc.).
Almacenamiento	Ataques genéricos en el almacenamiento de datos y dispositivos (disco duro o disco de estado sólido [SSD]).

RIESGO DE CONECTIVIDAD DE RED NO AUTORIZADO

VECTOR	RIESGO
Email	Transmisión de datos simple a compleja (incluidos archivos grandes).
SMS	Transmisión de datos simple, comando limitado y facilidad de control (comando de servicio).
HTTP get/post	Vector de ataque genérico para conectividad basada en navegador, comando y control.
TCP/UDP socket	Vector de ataque de nivel inferior para transmisión de datos simple a compleja.
Exfiltración DNS	Vector de ataque de nivel inferior para una transmisión de datos simple a compleja, lenta pero difícil de detectar.
Bluetooth	Transmisión de datos simple a compleja, comando basado en perfil y facilidad de control, vector de ataque genérico para proximidad.
WLAN/WiMAX	Vector de ataque genérico para el comando y control completo del objetivo, equivalente a la red cableada.

FUGAS DE DATOS CONFIDENCIALES

1. La cantidad de espacio de almacenamiento que se encuentra en muchos dispositivos está creciendo y, en promedio, casi cualquier dispositivo pronto será capaz de almacenar varios gigabytes de datos.
2. Esto aumenta el riesgo de fuga de datos, particularmente cuando los dispositivos móviles almacenan información replicada de las redes empresariales.
3. La fuga de datos confidenciales puede ser involuntaria.
4. Los ataques de canal lateral durante períodos prolongados permiten la creación de un perfil de usuario detallado en términos de movimientos, comportamiento y hábitos privados / comerciales.
5. Los usuarios que pueden ser considerados en riesgo pueden requerir protección física adicional.

RIESGO ASOCIADO CON EL ALMACENAMIENTO Y LA TRANSMISIÓN DE DATOS MÓVILES.

El uso de dispositivos móviles a menudo aumenta el riesgo asociado con el almacenamiento y la transmisión inseguros.

Almacenamiento de datos confidenciales inseguros
• Las aplicaciones pueden almacenar datos confidenciales como credenciales o fichas como texto sin formato. • Los datos almacenados por el usuario a menudo se replican sin cifrado. Los archivos estandarizados, como presentaciones y hojas de cálculo, se almacenan sin cifrar para un acceso rápido y conveniente. • Los dispositivos móviles a menudo están asociados con el almacenamiento en la nube, lo que a su vez agrega riesgo.

Transmisión de datos confidenciales inseguras
• Los dispositivos móviles dependen principalmente de la transmisión inalámbrica de datos, creando un riesgo de conectividad de red no autorizada, particularmente cuando se utiliza una LAN inalámbrica. • Es probable que los usuarios utilicen redes públicas no seguras para la transmisión de datos. • El reconocimiento automático de red, una característica común en los sistemas operativos móviles, puede vincularse a las WLAN disponibles en las cercanías, memorizar identificadores de conjunto de servicios (SSID) y canales y allanar el camino para ataques gemelos malvados.

VULNERABILIDADES DE CONDUCCIÓN

La naturaleza restringida de las aplicaciones de dispositivos móviles aumenta el riesgo de ataques automáticos.

El tamaño del dispositivo móvil restringe las capacidades de visualización y edición.

El software de procesamiento de textos, hojas de cálculo y presentaciones está optimizado para abrir y leer solamente, pero los documentos pueden contener hipervínculos activos, macros y documentos incrustados.

Esto se conoce como un vector de ataque para malware y otras vulnerabilidades. Es posible que las aplicaciones móviles no reconozcan enlaces mal formados o proporcionen advertencias adecuadas a los usuarios.

Los usuarios pueden verse perjudicados por la inserción de material ilegal, el uso accidental de servicios "Premium" a través de SMS / MM o la omisión de los mecanismos de autenticación.

TEMA 4:

Consumerización de TI y dispositivos móviles

La consumerización o consumidorización es una tendencia creciente en la cual las nuevas tecnologías de la información surgen primero en el mercado del consumidor y luego se propagan hacia las organizaciones comerciales y gubernamentales.

CONSUMERIZACIÓN DE TI

La consumerización de TI es la reorientación de tecnologías y servicios diseñados en torno al usuario final individual. Ejemplos incluyen:

- Dispositivos inteligentes como teléfonos inteligentes y tabletas.
- Estrategias BYOD.
- Nuevas aplicaciones y servicios disponibles gratuitamente.
- La consumerización no se limita a los dispositivos.
- Las nuevas aplicaciones y servicios disponibles de forma gratuita brindan mejores experiencias de usuario para cosas como tomar notas, videoconferencias, correo electrónico y almacenamiento en la nube que sus respectivas contrapartes aprobadas por la empresa.
- En lugar de recibir dispositivos y software emitidos por la compañía, los empleados utilizan cada vez más sus propias soluciones que se adaptan a su estilo de vida, necesidades y preferencias del usuario.

TRAE TU PROPIO DISPOSITIVO

El uso de dispositivos móviles de propiedad privada para fines laborales se ha consolidado rápidamente.

Esta tendencia es tanto positiva como negativa.

La desventaja es la proliferación de dispositivos con riesgo de seguridad conocido (o desconocido), y el desafío formidable de administrar la seguridad del dispositivo contra varias incógnitas.

BYOD se está convirtiendo en un importante factor de motivación laboral, porque los empleados ya no están dispuestos a aceptar restricciones tecnológicas.

PROS Y CONTRAS DE BYOD

PROS	CONTRAS
• Cambia los costos al usuario. • Satisfacción del trabajador. • Actualizaciones de hardware más frecuentes. • Tecnología de vanguardia con las últimas características y capacidades.	• Pérdida de control de TI. • Riesgo de seguridad conocido o desconocido. • La política de uso aceptable es más difícil de implementar. • Cumplimiento y propiedad poco claros de los datos.

INTERNET DE LAS COSAS

El Internet de las cosas (IoT) se refiere a objetos físicos que poseen elementos integrados de red y computación y se comunican con otros objetos a través de una red. Aunque el riesgo específico depende del uso, IoT crea varios tipos de riesgo.

Riesgo del negocio	Riesgo operacional	Riesgo técnico
• Salud y seguridad. • Cumplimiento normativo. • Privacidad del usuario • Costos inesperados	• Acceso inapropiado a la funcionalidad. • Uso de la sombra. • Desempeño.	• Vulnerabilidades del dispositivo. • Actualizaciones de dispositivos. • Gestión de dispositivos

BIG DATA

Big data es tanto un término técnico como de marketing que se refiere a un activo empresarial valioso: la información.

Big data se basa en conjuntos de datos que son demasiado grandes o que cambian demasiado rápido para ser analizados utilizando técnicas tradicionales de bases de datos o herramientas de software comúnmente utilizadas.

El cambio en las capacidades analíticas que se ocupan de big data puede introducir riesgos técnicos y operativos, que incluyen:

- Impacto técnico amplificado: conjuntos de datos más grandes están en peligro si son atacados.
- Privacidad en la recopilación de datos: las personas pueden sentir que la información revelada es demasiado intrusiva.
- Re identificación: durante la agregación, la información semi-anónima puede convertirse en información identificable, comprometiendo la privacidad individual.

TEMA 5:

Colaboración en la nube y digital

COMPUTACIÓN EN LA NUBE

El NIST define la "computación en la nube" como un "modelo para permitir el acceso conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de gestión o interacción del proveedor de servicios ".

La computación en la nube ofrece a las empresas una forma de ahorrar en el gasto de capital asociado con los métodos tradicionales de gestión de TI.

Las plataformas comunes que se ofrecen en la nube incluyen:

- Software como servicio (SaaS)
- Plataforma como servicio (PaaS)
- Infraestructura como servicio (IaaS)

PRINCIPALES AMENAZAS DE COMPUTACIÓN EN LA NUBE

El riesgo relacionado con la computación en la nube puede conducir a una serie de diferentes eventos de amenaza. Cloud Security Alliance enumera las siguientes amenazas principales de computación en la nube:

- Violaciones de datos.
- Pérdida de datos.
- Secuestro de cuenta.
- Interfaces de programación de aplicaciones (API) inseguras.
- Denegación de servicio (DoS).
- Usuarios internos maliciosos.
- Abuso de servicios en la nube.
- Diligencia debida insuficiente.
- Problemas tecnológicos compartidos

APLICACIONES WEB

Las empresas a menudo usan las ofertas de SaaS, a veces extendiendo este uso a procesos comerciales críticos y aplicaciones relacionadas.

Estas ofertas de servicios brindan ventajas comerciales, pero también generan vulnerabilidades de flujo de datos que pueden ser explotadas por el ciber crimen y la guerra cibernética.

SaaS aumenta el riesgo en la capa de aplicación, incluidos estos vectores de ataque:

- Hazañas de día cero
- Malware primario
- Malware secundario

REDES SOCIALES

La tecnología de redes sociales implica la creación y difusión de contenido a través de las redes sociales a través de Internet.

El uso de las redes sociales ha creado plataformas de comunicación altamente efectivas donde cualquier usuario, prácticamente en cualquier parte del mundo, puede crear contenido libremente y difundir esta información en tiempo real a una audiencia global.

Las empresas están utilizando las redes sociales para aumentar el reconocimiento de marca, las ventas, los ingresos y la satisfacción del cliente; sin embargo, existe un riesgo asociado con su uso.

RIESGOS DEL USO EMPRESARIAL DE LAS REDES SOCIALES

Los riesgos asociados con una presencia corporativa en las redes sociales incluyen:

- Introducción de virus / malware a la red organizacional.
- Información errónea o información engañosa publicada a través de una presencia corporativa fraudulenta o secuestrada.
- Derechos de contenido poco claros o indefinidos a la información publicada en sitios de redes sociales.
- Insatisfacción del cliente debido a un aumento esperado en la calidad / puntualidad de la respuesta del servicio al cliente.
- Mal manejo de las comunicaciones electrónicas que pueden verse afectadas por las regulaciones de retención o el descubrimiento electrónico.

RIESGOS DEL USO DE LAS REDES SOCIALES POR PARTE DE LOS EMPLEADOS

Los riesgos asociados con el uso personal de los empleados de las redes sociales incluyen:

- Uso de cuentas personales para comunicar información relacionada con el trabajo.
- Publicación de fotografías o información por parte de los empleados que las vinculen con la empresa.
- Uso excesivo por parte de los empleados de las redes sociales en el lugar de trabajo.
- Acceso de los empleados a las redes sociales a través de dispositivos móviles suministrados por la empresa (teléfonos inteligentes, tabletas).

MUCHAS GRACIAS