¿Para qué me sirve conocer los delitos informáticos si soy Archivista?

Lic. Ing. Roberto Lemaître P.
Abogado-Ingeniero Informático

XXXI CONGRESO ARCHIVÍSTICO NACIONAL

LA INFORMACIÓN: EL ADN DE LA TRANSFORMACIÓN DIGITAL

ARCHIVO NACIONAL
COSTA RICA

26 DE ENERO 2017

- *Finalmente, el **26 de Enero de 1993** se interconecta una docena de nodos ubicados en la Unidad de Redes, Centro de Informática, Escuela de Geología y Escuela de Física de la Universidad de Costa Rica con la **Internet,** utilizando el Punto de Presencia (PoP) de NSF en Homestead y un enrutador CISCO IGS en préstamo por la Universidad de Wisconsin.*

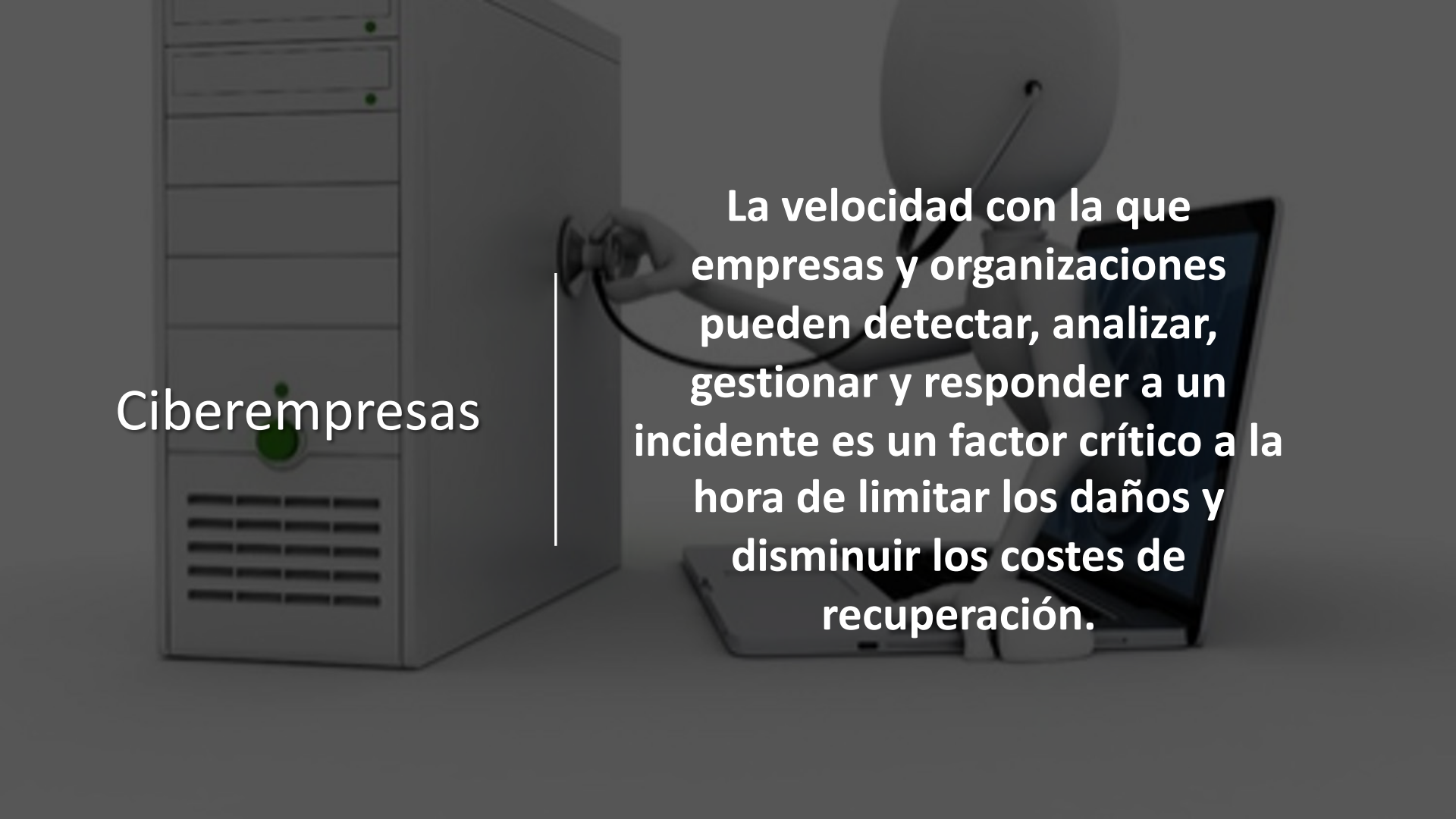
- ***26 años** de la Primera Conexión a la Internet en Costa Rica*

Ciberempresas

Los mesías cibernéticos no existen

Los incidentes de seguridad informática son reales y hay que desarrollar mecanismos para poder gestionarlos correctamente.

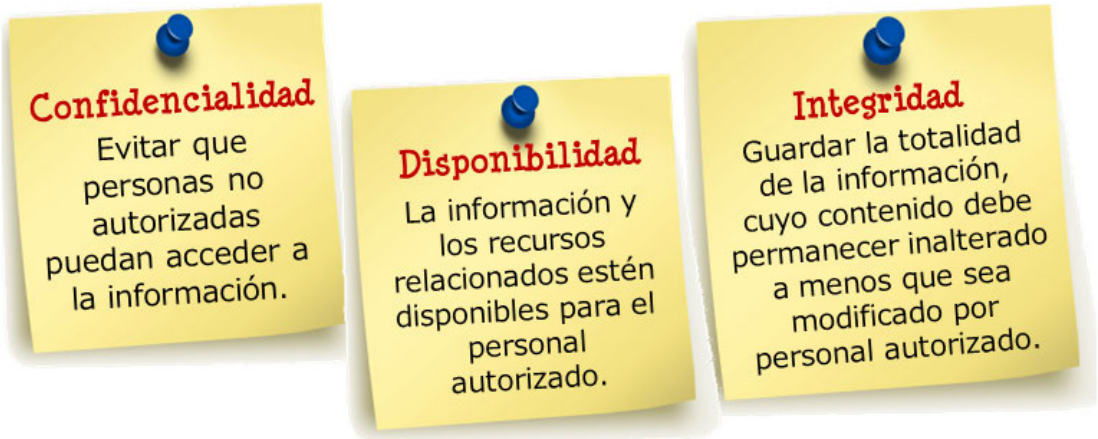
Es necesario ser conscientes y aceptar que no existe la seguridad total.



Ciberempresas

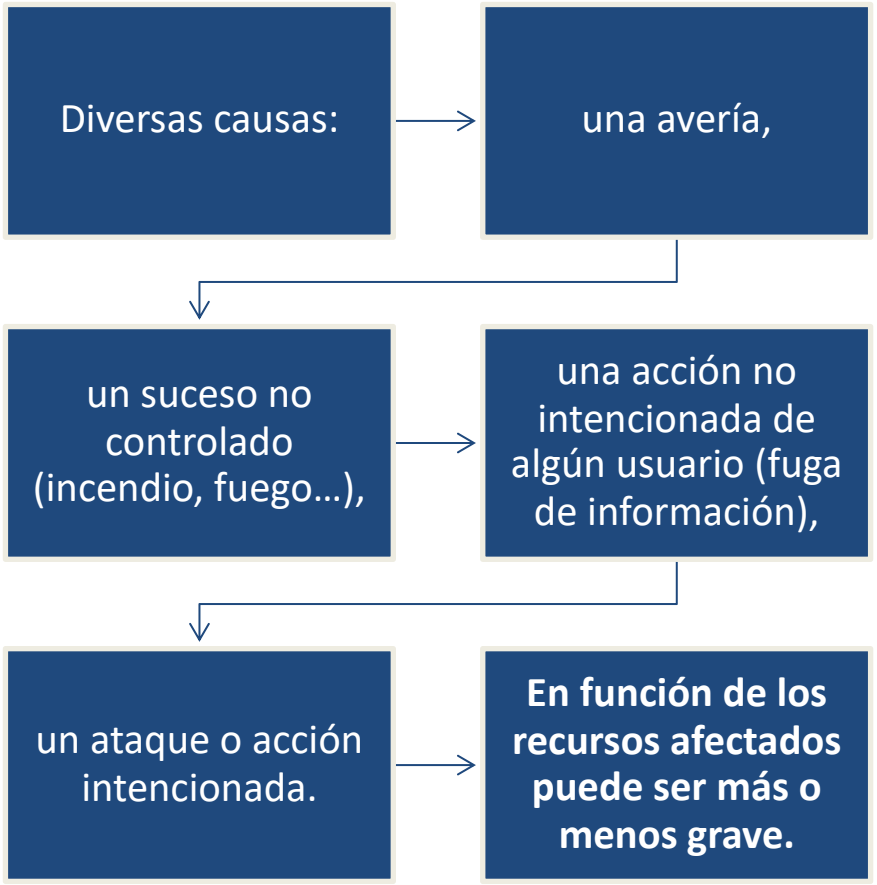
La velocidad con la que empresas y organizaciones pueden detectar, analizar, gestionar y responder a un incidente es un factor crítico a la hora de limitar los daños y disminuir los costes de recuperación.

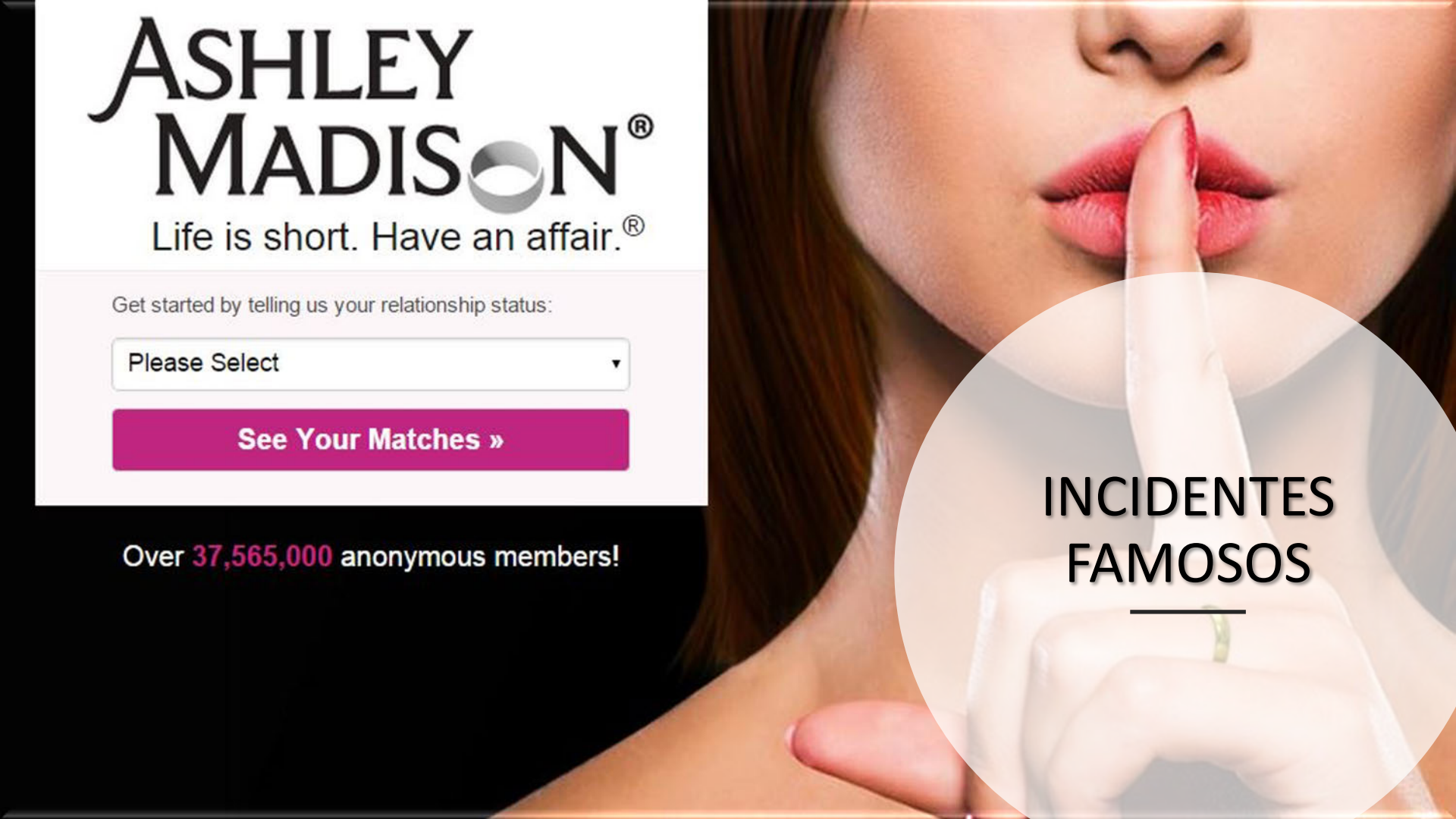
INCIDENTE



Cualquier suceso que puede afectar negativamente a alguno de los aspectos de la seguridad de la información de la empresa:

¿Cómo ocurren?




ASHLEY MADISON®
Life is short. Have an affair.®
Get started by telling us your relationship status:
Please Select
See Your Matches »
Over 37,565,000 anonymous members!
INCIDENTES FAMOSOS

El caso Ashley Madison: el 'hackeo' que desnudó a 39 millones de infieles

Este es el infierno que viven hoy los casi 39 millones de cibernautas que alguna vez se atrevieron a registrarse en Ashley Madison, el sitio más popular para contactarse con otras personas dispuestas a tener aventuras extramaritales bajo una presunción de absoluta confidencialidad.

Fuente:
https://www.nacion.com/tecnologia/internet/el-caso-ashley-madison-el-hackeo-que-desnudo-a-39-millones-de-infieles/7QWUS3A4SNDQDLICN4YJANGGHU/story/

Roban documentos militares clasificados porque nadie cambió la contraseña del router

Investigadores de seguridad han descubierto que documentos militares de la Fuerza Aérea de Estados Unidos, la Armada y el Pentágono han sido filtrados accidentalmente debido a que nadie cambió el usuario o la contraseña de una serie de routers.

Según uno de los expertos, los cibercriminales aprovecharon una vulnerabilidad en algunos modelos de routers Netgear, ***cuyas credenciales por defecto están disponibles en la web del fabricante, y la compañía desde hace dos años*** *advierte a todos sus usuarios que lo primero que hagan al instalar el router sea cambiar la contraseña.*

Fuente: ***https://es.gizmodo.com/roban-documentos-militares-clasificados-porque-nadie-ca-1827519507***

Eset Security: 69% de empresas de la región sufrieron al menos un incidente de inseguridad informática

GRÁFICO 2.1 *Incidentes de seguridad en empresas de Latinoamérica (2016)*

Eset Security: 69% de empresas de la región sufrieron al menos un incidente de inseguridad informática

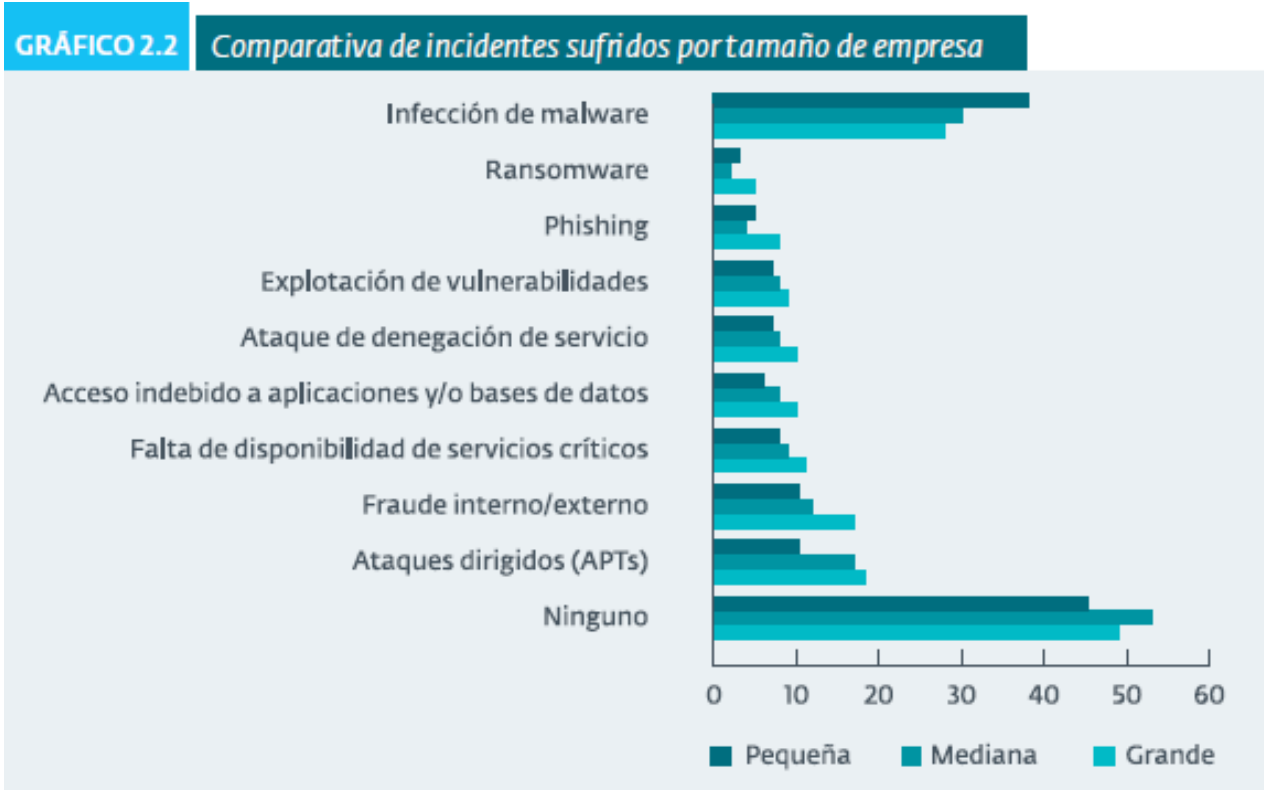
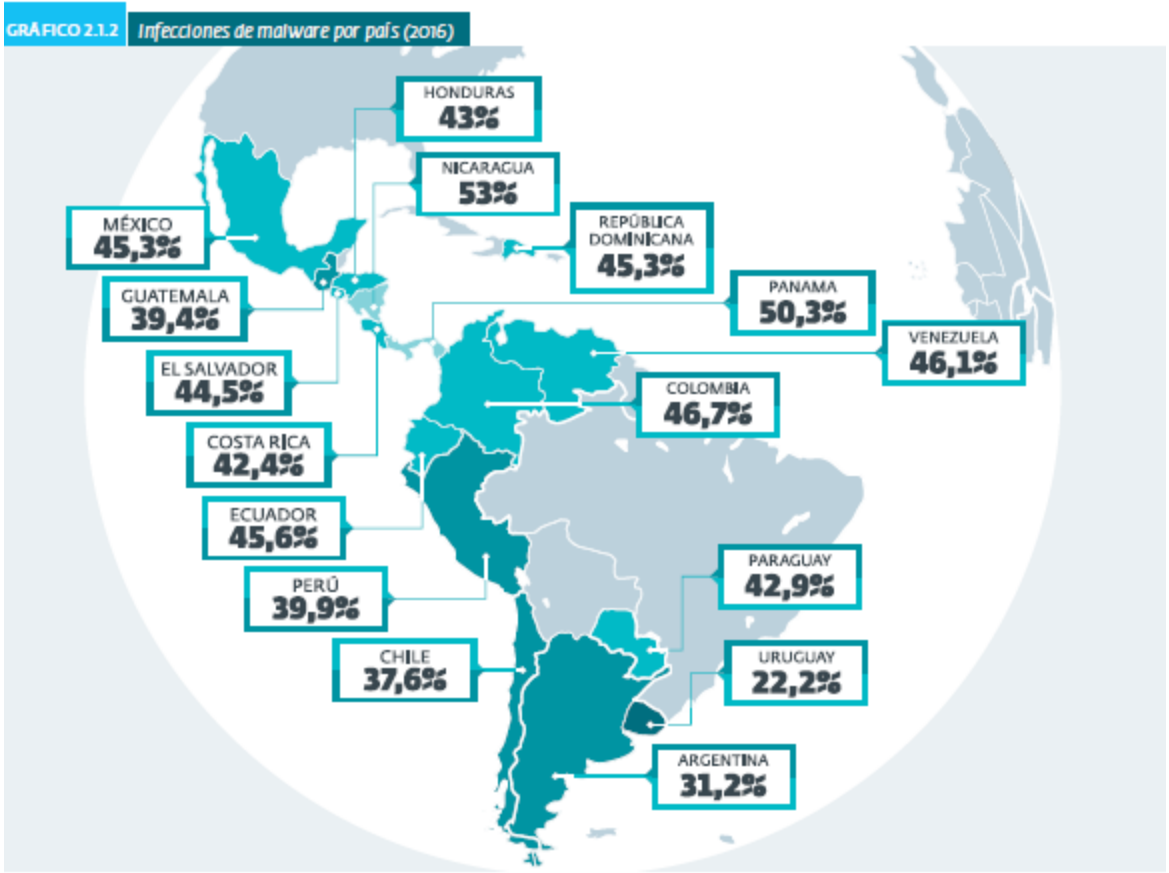


GRÁFICO 2.1.2 *Infecciones de malware por país (2016)*



¿ Y el gasto en ciberseguridad?

- El gasto de las empresas en ciberseguridad alcanzó en el año 2018 los 96.300 millones de dólares (79.773 millones de euros), según un estudio de la consultora Gartner, Inc.
- Esta cifra supone un aumento del 8 por ciento con respecto a 2017. El informe cita como causas de este incremento el hecho de que las organizaciones están gastando más en seguridad como resultado de regulaciones, cambio de mentalidad del comprador, conciencia de las amenazas emergentes y la evolución hacia estrategia de negocios.

¿ Y el gasto en ciberseguridad?

A juicio de las empresas, los incidentes de seguridad más frecuentes son el malware y el spam en los ordenadores,mientras que en dispositivos móviles son el robo y la pérdida de los mismos.

- Los incidentes de seguridad pueden provocar la interrupción del negocio. Estos son debidos principalmente a la caída o avería de los sistemas, una caída de las aplicaciones informáticas, o la falta de servicio o suministro por parte de los proveedores.

- Las infecciones por malware y la recepción de spam son los incidentes más reportados.

¿ Y el gasto en ciberseguridad?

- En cuanto a dispositivos móviles, una gran mayoría afirma no haber tenido percances de seguridad durante el último año. El robo y pérdida del terminal es lo más frecuente.

- Un alto porcentaje de las pymes afirma no haber sufrido ningún incidente de seguridad en el último año. Disponer de personal interno de seguridad incide de manera directa en la percepción de este tipo de incidentes.

¿ Y el gasto en ciberseguridad?

Tras un incidente, la mayoría de las empresas identifican las consecuencias más visibles, pero dejan de lado las consecuencias de carácter más técnico. En este campo, las reacciones son todavía muy limitadas.

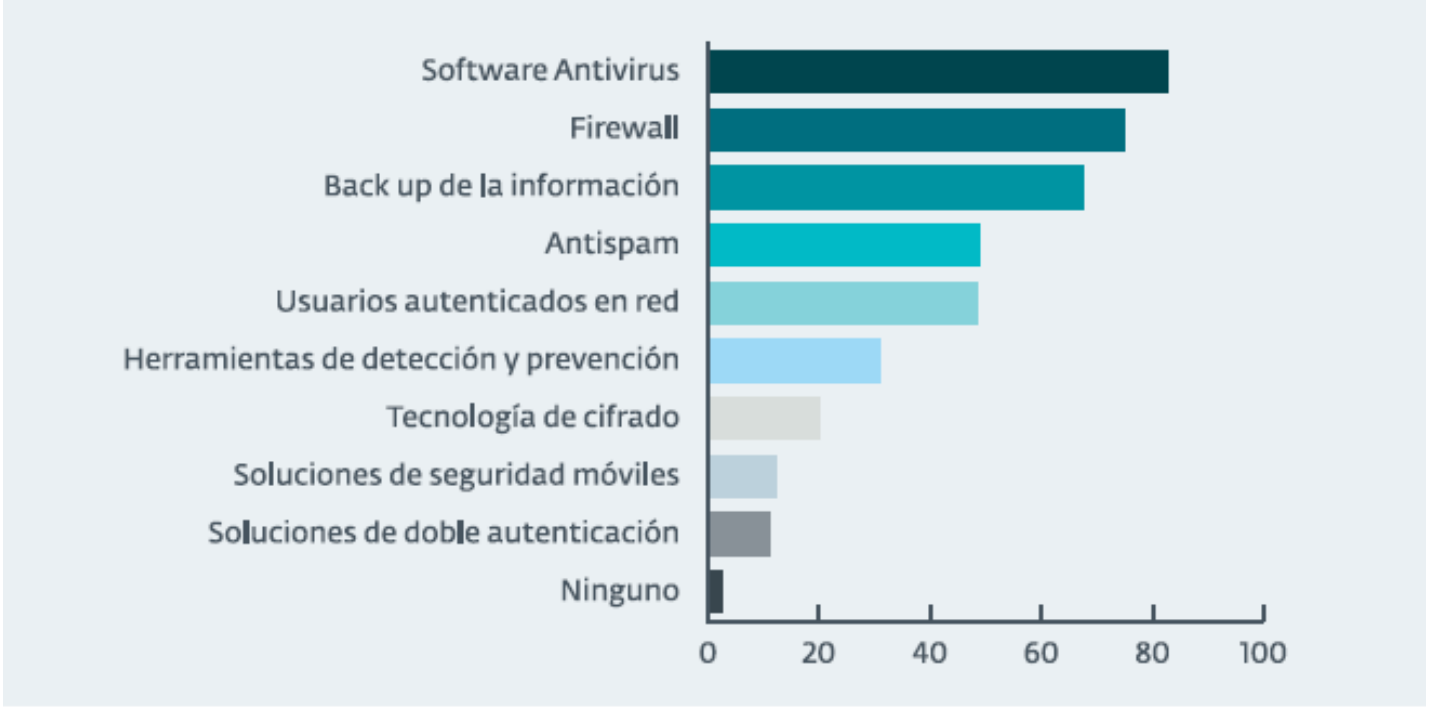
- Entre las pymes que han sufrido impactos negativos en su negocio, imagen o economía, a consecuencia de un incidente de seguridad,los incidentes con mayor ocurrencia son los que afectan al tiempo de trabajo,así como los que implican problemas de conexión o redes.
- Un gran porcentaje de las pymes no tiene definida una política de seguridad TIC, y las que lo han aplicado,lo han hecho recientemente

¿CÓMO RESPONDER ANTE UN INCIDENTE DE SEGURIDAD?

- Los datos arrojados por las encuestas demuestran que los controles de seguridad más implementados en Latinoamérica son el antivirus (83%), el firewall (75%) y el backup de la información (67%).

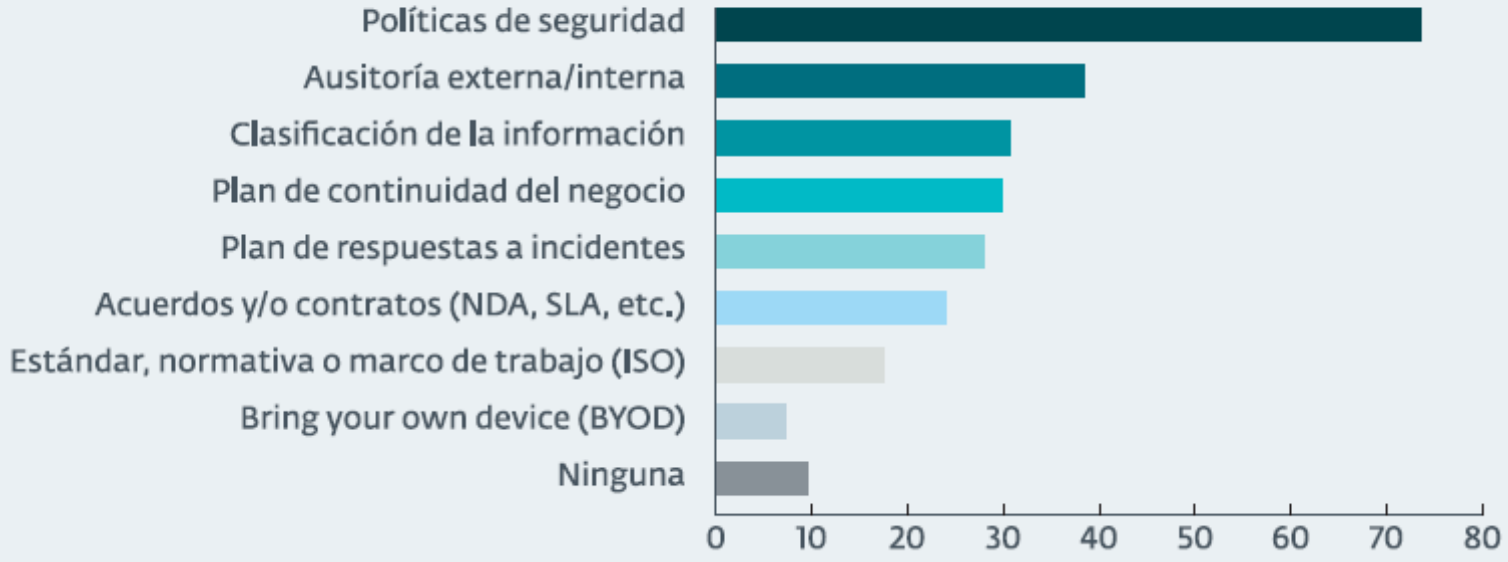
¿CÓMO RESPONDER ANTE UN INCIDENTE DE SEGURIDAD?

GRÁFICO 3.1.1 *Controles de seguridad más implementados en Latinoamérica durante 2016*



¿CÓMO RESPONDER ANTE UN INCIDENTE DE SEGURIDAD?

GRÁFICO 3.2.1 *Prácticas de gestión de la seguridad más implementadas en 2016 en Latinoamérica*




La respuesta
jurídica

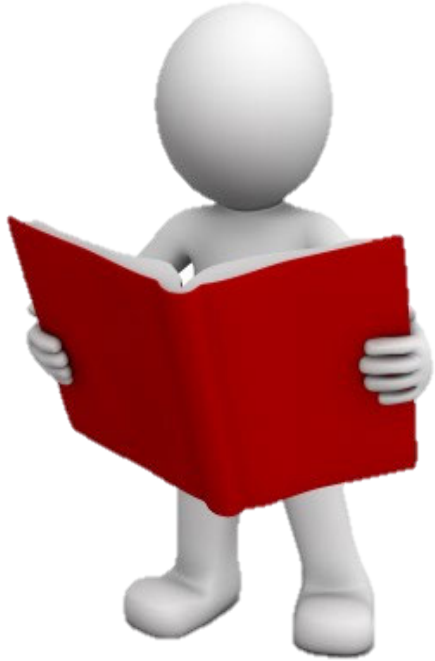
Ley de protección de la persona frente al tratamiento de sus datos personales Ley N. 8968 y su Reglamento

Protección de Datos

- **Artículo 1.- Objetivo y fin**
- Respeto a sus derechos fundamentales: **derecho a la autodeterminación informativa**
- **Su vida o actividad privada**
- **Defensa de su libertad e igualdad**

Protección de Datos

- Derechos de la persona



- **Acceso** de sus datos personales
- **Rectificación** o **supresión**
- **Consentir la cesión** de sus datos

Ley de Certificados, Firmas Digitales y Documentos Electrónicos y su Reglamentos

- La firma digital es una solución tecnológica que permite autenticar el origen y verificar la integridad del contenido de un mensaje de manera tal que ambas características sean demostrables ante terceros.

Ley de Certificados, Firmas Digitales y Documentos Electrónicos y su Reglamentos

- Propiedades:

✓ **Autenticidad:** El emisor es quien dice ser.

✓ **Integridad:** El documento No se ha modificado

✓ **No Repudio:** El emisor no puede negar la autoría

Código Penal

Artículo 196.- Violación de correspondencia o comunicaciones

Será reprimido con pena de prisión de uno a tres años a quien, con peligro o daño para la intimidad o privacidad de otro, y sin su autorización, se apodere, acceda, modifique, altere, suprima, intervenga, intercepte, abra, entregue, venda, remita o desvíe de su destino documentación o comunicaciones dirigidas a otra persona.

Artículo 196.- Violación de correspondencia o comunicaciones

La misma sanción indicada en el párrafo anterior se impondrá a quien, con peligro o daño para la intimidad de otro, utilice o difunda el contenido de comunicaciones o documentos privados que carezcan de interés público.

La misma pena se impondrá a quien promueva, incite, instigue, prometa o pague un beneficio patrimonial a un tercero para que ejecute las conductas descritas en los dos párrafos anteriores.

Artículo 196.- Violación de correspondencia o comunicaciones

La pena será de dos a cuatro años de prisión si las conductas descritas en el primer párrafo de este artículo son realizadas por:

a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.

Artículo 196.- Violación de correspondencia o comunicaciones

La pena será de dos a cuatro años de prisión si las conductas descritas en el primer párrafo de este artículo son realizadas por:

b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Artículo 196 bis.- Violación de datos personales

Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.

Artículo 196 bis.- Violación de datos personales

La pena será de dos a cuatro años de prisión cuando las conductas descritas en esta norma:

a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

b) La información vulnerada corresponda a un menor de edad o incapaz.

c) Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.

Artículo 229 bis.- Daño informático

Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable.

Artículo 229.- Daño agravado

Se impondrá prisión de seis meses a cuatro años:
[…]

6) Cuando el daño recayera sobre redes, sistemas o equipos informáticos, telemáticos o electrónicos, o sus componentes físicos, lógicos o periféricos.

Artículo 229 ter.- Sabotaje informático

Se impondrá pena de prisión de tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

La pena será de cuatro a ocho años de prisión cuando:

a) Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.

b) La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

c) El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas.

d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.

Artículo 230.- Suplantación de identidad

Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información.

Artículo 231.- Espionaje informático

Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio.

Artículo 232.- Instalación o propagación de programas informáticos maliciosos

Será sancionado con prisión de uno a seis años quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos.

Artículo 233.- Suplantación de páginas electrónicas

Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.

La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.

Artículo 234.- Facilitación del delito informático

Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos.

Artículo 236.- Difusión de información falsa

Será sancionado con pena de **tres a seis años** de prisión quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.

Metodología para la gestión de incidentes

FASE 1: PREPARACIÓN:

El primer paso consiste en **estimar las necesidades para la gestión de incidentes**.

Metodología para la gestión de incidentes

- **FASE 1: PREPARACIÓN:**

- Personal que va a realizar la gestión de incidentes.
- Documentación de los sistemas y redes que se usan en la empresa:

  Definir cuál es la actividad «normal» para permitir detectar actividades sospechosas que sean indicios de incidentes.

Metodología para la gestión de incidentes

- **FASE 1: PREPARACIÓN:**

  Registrar los contactos de terceras partes.

  Por ejemplo, si tenemos una web que la mantiene un proveedor, en caso de incidencia hay que tener identificado el responsable en el proveedor.

- Centros de respuesta ante incidentes de organismos externos en los que apoyarnos para la gestión de incidentes: CERT/CSIRT.

Metodología para la gestión de incidentes

- **FASE 1: PREPARACIÓN:**

Establecimiento de procedimientos de gestión:

- Las buenas prácticas señalan la necesidad de definir una **política de gestión de incidentes**, así como el **procedimiento** aseguir en caso de que ocurran.
- También, es recomendable tener un **catálogo con las incidencias** que tengan mayor probabilidad de ocurrir o mayor impacto previsible en la empresa,de forma que podamos predefinir pautas de actuación en caso de materializarse.

Metodología para la gestión de incidentes

FASE 2: DETECCIÓN Y ANÁLISIS

Es evidente que no se podrá gestionar un incidente si éste no se ha detectado.

Metodología para la gestión de incidentes

FASE 2: DETECCIÓN Y ANÁLISIS

Signos indicadores: son aquellos que ponen de manifiesto que un incidente ha ocurrido o puede estar ocurriendo,porejemplo:

- Alertas de sensores de un servidor
- Una alerta del antivirus
- La caída de un servidor o sistema
- Accesos lentos

Metodología para la gestión de incidentes

FASE 2: DETECCIÓN Y ANÁLISIS

Signos precursores: son los que nos pueden indicar que un incidente tiene posibilidades de ocurrir en el futuro, por ejemplo:

- La detección de un escáner depuertos
- El resultado del análisis de vulnerabilidades
- Las amenazas de ataque por parte de cibercriminales

Metodología para la gestión de incidentes

FASE 2: DETECCIÓN Y ANÁLISIS

Clasificación y priorización de incidentes

Una vez detectado un incidente, hay que **clasificarlo.** Se pueden usar para la clasificación, los siguientes **atributos**:

- **Tipo de amenaza**: código dañino, intrusiones, fraude, etc.
- **Origen de la amenaza**: interna o externa.
- La **categoría** de seguridad o **criticidad** de los sistemas afectados.
- El perfil de los **usuarios afectados**, su posición en la estructura organizativa de la entidad y, en su consecuencia,sus privilegios de acceso a información sensible o confidencial.
- El **número y tipología** de los sistemas afectados

Metodología para la gestión de incidentes

FASE 2: DETECCIÓN Y ANÁLISIS

Clasificación y priorización de incidentes

Las características del incidente, tipo de recursos afectados y criticidad de los mismos determinará el impacto potencial sobre el negocio de la empresa, además del orden de prioridad en el tratamiento, en caso de detectarse más de un incidente de forma simultánea.

Metodología para la gestión de incidentes

Level I	Resuscitation	see patient immediately
Level II	Emergency	within 15 minutes
Level III	Urgency	within 30 minutes
Level IV	Less Urgency	within 60 minutes
Level V	Non Urgency	within 120 minutes

Metodología para la gestión de incidentes

FASE 2: DETECCIÓN Y ANÁLISIS

Metodología para la gestión de incidentes

FASE 2: DETECCIÓN Y ANÁLISIS

Notificación del incidente

El proceso de notificación de incidentes de seguridad pasa por las siguientes acciones:**reportar, notificar y registrar el incidente e iniciar el seguimiento en un evento de gestión**. En función del tipo de incidente,éste se asignará y escalará a las personas que procedan para asegurar, en la medida de lo posible, su análisis, resolución y cierre.

Metodología para la gestión de incidentes

FASE 3: CONTENCIÓN, RESOLUCIÓN Y RECUPERACIÓN

- Las estrategias de contención de incidentes varían dependiendo del tipo de incidente, así como del posible impacto sobre la empresa.
- En función de la **gravedad** de los incidentes, puede que sea necesario aplicar medidas como deshabilitar servicios, apagar sistemas o desconectarlos de la red, para intentar evitar que el incidente se extienda por la empresa.
- Estas decisiones pueden facilitarse y agilizarse si se han **definido previamente estrategias y procedimientos** para contener los distintos tipos de incidentes posibles.

Metodología para la gestión de incidentes

FASE 3: CONTENCIÓN, RESOLUCIÓN Y RECUPERACIÓN

- Una vez contenido el incidente, hay que **verificar si es necesario** eliminar o limpiar componentes asociados al incidente, además de proceder a la **recuperación de todos los sistemas afectados**, para devolverlos a la situación de operación normal de la empresa.

- En las actividades de recuperación se realiza la **eliminación de los componentes asociados al incidente** y otras actividades que se consideren adecuadas de cara a resolver el incidente o prevenir que vuelva a ocurrir en el futuro.

Metodología para la gestión de incidentes
FASE 3: CONTENCIÓN, RESOLUCIÓN Y RECUPERACIÓN

Actividades de resolución:

- Instalación de parches de seguridad
- Cambios en el cortafuegos*(firewall)*
- Cambios en las listas de acceso

Actividades de recuperación:

- Restaurar información desde las copias de seguridad *(backups)*
- Reemplazar componentes afectados con otros limpios de infección
- Instalar actualizaciones de software
- Cambiar contraseñas
- Reforzar la seguridad actualizando reglas del cortafuegos

Metodología para la gestión de incidentes

FASE 4: ACCIONES POSTERIORES AL CIERRE

- El cierre de un incidente de seguridad y el fin de su gestión debe incluir un conjunto de evidencias que acrediten las acciones que se han llevado a cabo, los procesos que se han realizado y todas las personas que han estado involucradas o han sido consultadas para su gestión.
- **Es recomendable disponer de un registro común para todos los incidentes**, donde se describan los datos mencionados anteriormente, incluyendo el origen y la persona que detecta el incidente, así como los servicios y sistemas infectados, fechas/horas más relevantes, responsables de la gestión y acciones tomadas.

Metodología para la gestión de incidentes

FASE 4: ACCIONES POSTERIORES AL CIERRE

- Periódicamente se deben analizar las actividades realizar, estudiando posibles mejoras o cambios a realizar ante futuros incidentes.
- Además, es recomendable recoger y analizar métricas sobre los tipos y frecuencia de incidentes, impactos (financieros, obligaciones legales, imagen frente a terceros, operativos), métodos de resolución, coste de la resolución de incidentes y acciones correctivas o preventivas.
- De esta forma, si es necesario, se pueden detectar mejoras en los procedimientos de gestión, escalamiento, etc.

Metodología para la gestión de incidentes

FASE 4: ACCIONES POSTERIORES AL CIERRE

1.Mantener un registro de los incidentes sufridos en tu negocio.

2.Hacer un seguimiento de las acciones realizadas y las personas que hayan intervenido en la gestión del incidente.

3.Mantener un registro de los documentos que sirvan como evidencia de las acciones realizadas para solucionar o cerrar el incidente de seguridad.

4.Mantener esta información como inventario de los incidentes de seguridad sufridos por mi negocio para intentar mejorar la gestión sobre mis activos implementando medidas que contribuyan a impedir que los incidentes de seguridad se repitan

Roberto Lemaître Picado
Abogado-Ingeniero Informático
Especialista en Delitos Informáticos
roberto.lemaitre@micit.go.cr
rolemaitre@protonmail.com
rolemaitre@abogados.or.cr

XXXI CONGRESO ARCHIVÍSTICO NACIONAL

LA INFORMACIÓN: EL ADN DE LA TRANSFORMACIÓN DIGITAL

ARCHIVO NACIONAL
COSTA RICA