GUÍA CYBER

BUENAS PRÁCTICAS EN PROTECCIÓN DE CIBERRIESGOS

PARA NO EXPERTOS

COMISIÓN DE TRABAJO
RIESGOS TECNOLÓGICOS

agers

BUENAS PRÁCTICAS EN PROTECCIÓN DE CIBERRIESGOS PARA NO EXPERTOS

agers

ISBN: 978-84-09-48685-4
Depósito Legal: M-5482-2023
Copyright: DEP638116228481427893
Nota Legal - Copyright

ÍNDICE

1. INTRODUCCIÓN

Las encuestas sobre los principales riesgos a los que se enfrentan las organizaciones sitúan en la mayoría de los casos en los primeros lugares al riesgo cibernético[1]. Se trata de un riesgo que además de preocuparnos exige que nos ocupemos. Y la ocupación comienza con la prevención. Sin esta, la probabilidad de sufrir un incidente significativo será importante, al igual que el impacto del mismo. Pero como por muchas medidas que tomemos para prevenir un incidente no podemos garantizar que este no se produzca debemos contar con medidas de detección, respuesta y recuperación para que el daño se contenga lo antes posible y con el menor impacto posible.

La transferencia del riesgo a través de pólizas de seguro nos permitirá disponer de servicios que nos pueden ayudar a gestionar el siniestro además de reducir o cancelar el impacto económico de este. Pero la transferencia del riesgo no será posible si no disponemos de medidas adecuadas para prevenir y responder ante incidentes tecnológicos.

Este es el objetivo de este trabajo. Trasladar fundamentalmente al colectivo de gerentes de riesgos y/o seguros, pero también a todo el personal no técnico implicado en estos riesgos, qué medidas de diversa índole son recomendables para gestionar la prevención de los incidentes cibernéticos.

Sin la implantación de una gran parte de estas medidas será muy difícil transferir al mercado asegurador estos riesgos y a veces, dependiendo del sector, será difícil aun implantándolas. Además, teniendo en cuenta las limitaciones que existen de capacidad y las elevadas primas de estos seguros, es bastante probable que de producirse un siniestro de magnitud los límites contratados se encuentren por debajo del coste total del siniestro. Por otra parte, teniendo en cuenta las elevadas franquicias que se aplican, es probable también gestionar algún siniestro que no quede cubierto en póliza, al no alcanzar la franquicia.

Esto debería hacer que el punto de partida para enfrentarnos a este riesgo sea abordarlo como si no tuviésemos seguro. Por un lado, porque si no hemos desarrollado una gran cantidad de medidas es bastante probable que no con-

[1] World Economic Forum Global Risks Perception Survey, 2022-2023.

sigamos que una aseguradora se interese por nuestro riesgo, por otro, porque probablemente los límites puedan ser insuficientes para siniestros de gran impacto, como un ataque exitoso de ransomware que afecte a bases de datos críticas en la operativa diaria de la organización.

Lo que nos devuelve a la importancia de gestionar estos riesgos para reducir su probabilidad de ocurrencia e impacto.

No pretendemos que con la lectura de este documento nos convirtamos en expertos, pero sí entender, uno, qué tipo de medidas se pueden aplicar y dos, los requisitos que una aseguradora exige para contratar estos seguros. En este sentido, el gerente de riesgos y/o seguros se debe convertir en un socio del departamento de seguridad de la información para trasladar a la alta dirección la importancia de dotarles de medios.

Hemos trabajado, uno, para comprender cuál es la información que solicitan las aseguradoras en los cuestionarios (o la que se comunica en los road shows) y conocer su importancia y dos, para trasladar estos conocimientos a este manual. Consideraremos que este trabajo ha sido satisfactorio si hemos aportado a alguno de los lectores un avance en esta materia.

2. AGRADECIMIENTOS

Comisión Riesgos Tecnológicos

El Corte Inglés	Juan Gayá – Coordinador
	África Sánchez
globalvia	Belén Medina
agers	Eva Pérez
	Elisa Mª Rojo
aena	Álvaro González
CEPSA	Juan Miguel García
	David Martínez
Sanitas	Ignacio Reclusa
Damm	Carme Kovács
noatum	Ana Ruiz
abertis	Juan Ramón Claver
MERCADONA	Isabel Hernández

Expertos que han colaborado

AIG	Olivier Marcen
AXA XL Insurance	Carlos Rodríguez Sanz
QBE	Luis Alonso Serrano
Liberty Seguros	Alvaro Menchen
HDI	Elena Leguina
TOKIO MARINE HCC	Sandra Da Silva
beazley	Ana Misol
Munich RE	Vallejo Moratalla Sara

3. QUÉ MODELO SEGUIR

Probablemente, si nos dedicamos al negocio de gestionar los riesgos y/o seguros conozcamos las medidas que pueden reducir el riesgo del fuego en un inmueble o en una planta de producción y entendamos los requisitos que requiere una aseguradora para aceptar la transferencia de este riesgo.

¿Pero nos pasa lo mismo con los riesgos digitales? La mayoría probablemente contestaríamos que no. Y tratándose del riesgo más importante al que nos enfrentamos en estos momentos, según prácticamente todas las encuestas, esa respuesta nos debería generar incomodidad.

Cómo hemos abordado este problema

Empezamos solicitando a distintas aseguradoras mantener una reunión en la que nos relacionaran los distintos elementos que consideraban importante tener implantados para aceptar estos riesgos. En general, con distinto orden, agrupación de preguntas o redacción, los conceptos eran similares. También preguntamos si había líneas rojas que automáticamente diesen lugar a rechazar un riesgo, y también con carácter general la respuesta era negativa: es el conjunto de respuestas a determinadas preguntas y las características del negocio las que generan líneas rojas, aunque algunas líneas rojas existen y las iremos destacando a lo largo del documento.

El segundo paso fue conocer metodologías relacionadas con este asunto. Fueron dos que acabaron atrayendo nuestro interés, la UNE-EN-ISO 27002 (Código de prácticas para los controles de seguridad de la información) y las llamadas popularmente como normas NIST (Marco para la mejora de la seguridad cibernética, desarrollado por el *National Institute of Standards and Technology*, una unidad del Departamento de Comercio de Estados Unidos).

Las segundas fueron las que entendimos que se ajustaban mejor a la información que recogimos de las aseguradoras. Además, este modelo agrupa las funciones en cinco habituales en la gestión de riesgos: IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER Y RECUPERAR.

Identificar – Desarrollar una comprensión organizacional para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades.

Proteger – Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos.

Detectar – Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética.

Responder – Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de seguridad cibernética.

Recuperar – Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética.

En este modelo cada una de estas funciones se desglosa en categorías. Sin embargo, en las próximas páginas, no hemos utilizado literalmente las que figuran en la NIST. Hemos eliminado algunas e incorporado otras, en base a los conocimientos recogidos en la etapa de análisis con las aseguradoras.

A continuación hemos querido describir, utilizando un lenguaje no técnico, las medidas que recoge cada categoría, explicando su importancia y en qué consiste.

Las preguntas que realizan las aseguradoras irán cambiando en el tiempo, en tanto que las herramientas que existen para proteger los sistemas van evolucionando para adaptarse a las nuevas técnicas de ataque pero los conceptos se mantienen estables. En muchos casos estos son similares al mundo físico: por ejemplo la sectorización que es una medida fundamental para reducir el daño de incendio tiene su equivalente en la segmentación (de redes, perfiles de acceso, etc.) para reducir el daño tecnológico.

4. BUENAS PRÁCTICAS PARA LA PROTECCIÓN DE RIESGOS CIBERNÉTICOS

A continuación se describen, agrupadas por las categorías (a las que hemos denominados FASES): IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER Y RECUPERAR las distintas buenas prácticas que pueden ser aplicadas para defenderse de los riesgos digitales.

Hemos incluido también una FASE 0, denominada CONOCIMIENTO DE LA EMPRESA, en la que se describen las características de la organización y del entorno en el que opera, y que será fundamental para la IDENTIFICACIÓN DEL RIESGO.

Para cada una de estas medidas se describe **en qué consiste y su aportación** para minorar el riesgo o limitar los daños si no se evita el riesgo.

Fase 0 Conocimientos de la empresa

Para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades la primea noción pasa por desarrollar una comprensión organizacional. La primera fase de esa comprensión es una **descripción de las características** de la propia organización y del **entorno** en que ésta opera.

Medidas

Información de la organización

Descripción de la organización

Una descripción de la organización que incluya al menos la siguiente información:

- Compañía.
- Actividad de la compañía.
- Perforados con lodos.
- Número de empleados, desglose por países.
- Número y descripción de situaciones de riesgo, desglose por países.
- Número y descripción de situaciones de riesgo, desglose por países.

Volumen de actividad/Facturación:

- desglose por actividades.
- desglose por países.
- porcentaje que representa la actividad online respecto del total.

Cotizada: Sí/No. En caso afirmativo mercado de cotización.

Organigrama societario.

Plan estratégico de la organización

La organización dispone de un plan estratégico que establece la posición de la organización en la cadena de suministro.

El plan estratégico se traduce en objetivos concretos, siendo tanto el plan y como los objetivos comunicados a la organización.

La organización cuenta con planes de contingencia para dar respuesta a situaciones inusuales.

Entorno empresarial

Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.

Se identifica y se comunica la función de la organización en la cadena de suministro así como en la infraestructura crítica y su sector industrial.

Se establecen y se comunican las prioridades para la misión, los objetivos y las actividades de la organización.

Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos. Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).

Fase 1 Identificación

Esta fase tiene como objetivo desarrollar una comprensión organizacional para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades.

Como en general las pólizas ciber cuentan con una cobertura de pérdida de beneficios, los aseguradores tienen interés en que sus asegurados dispongan de una cultura que les permita instruir a la organización para ejercer acciones preventivas y realizar un ejercicio de *loss prevention*.

Contar con una cultura de análisis, control y prevención, definiendo qué, quién y cómo se ha de ejecutar la misma, así como de qué manera las partes han de ser informadas, involucradas y desempeñarse, permite a la organización adelantarse y actuar con perspectiva.

Medidas

Gestión de activos

Existe un inventario de los activos

En la fase de identificación, la gestión de los activos pasa por dos elementos críticos:

- La existencia de un **inventario de activos.**
- La **identificación de la propiedad** de los activos inventariados.

El inventario de los activos incluye **los datos, el personal, los dispositivos, los sistemas y las instalaciones** que permiten a la organización alcanzar los objetivos empresariales. En el inventario, los activos están **priorizados en función de su criticidad** de modo que se identifican y se administran de forma coherente con su importancia relativa **para los objetivos organizativos y la estrategia de riesgos** de la organización.

Sin ser una lista cerrada, **el inventario de activos incluye** al menos:

- Los dispositivos y sistemas físicos:
  - Los servidores y su configuración.
  - Los puestos de trabajo (sobremesa y portátiles) y su configuración.
  - Teléfonos móviles.
- Las aplicaciones informáticas y las plataformas de *software* utilizadas en la organización.
- La red de comunicaciones (WAN y LAN).
- Las dependencias en las que se desarrolla la actividad.
- Los activos intangibles con valor para la organización, respecto de los cuales habrá que:
  - inventariar y clasificar la información.
  - mapear la comunicación organizacional y los flujos de datos.
  - catalogar los sistemas de información externos.
- Los activos críticos.

Línea Roja Mercado Asegurador: Disponer de un inventario de activos críticos que los suscriptores puedan revisar es básico para poder tener cobertura.

Existe priorización de los recursos

Existen reglas claras y conocidas por todos los actores de la organización para la priorización de los recursos (*hardware*, dispositivos, datos, tiempo, personal y *software*) en función de su clasificación, criticidad y valor comercial.

Existe una asignación de los roles y las responsabilidades

La asignación de roles y responsabilidades en materia de ciberseguridad para todos los actores de la organización y para los terceros interesados (proveedores, clientes, socios externos) es clara y conocida por todos ellos.

Gobernanza

La compañía tiene una política de ciberseguridad

La política de ciberseguridad es centralizada para toda la organización independientemente de la ubicación, razón social… incluyendo los roles de cada miembro de la organización.

La máxima responsabilidad de ciberseguridad en la organización recae en un miembro de la alta dirección.

La política es comunicada, revisada y notificada a toda la organización.

La política tiene en cuenta los requisitos legales del entorno de la organización.

Existe un presupuesto destinado a ciberseguridad y éste se gestiona.

El personal recibe formación y concienciación sobre ciberseguridad periódicamente, auditándose regularmente.

Línea Roja Mercado Asegurador: La formación de empleados, incluyendo herramientas de e-learning, campañas de phising, ejercicios de gestión de crisis o alertas de email, será uno de los puntos en los que los aseguradores podrán su foco.

Evaluación de riesgos

Existe una metodología de evaluación de riesgos que contempla y gestiona:

- Las vulnerabilidades a que se somete cada activo.
- Las amenazas tanto internas como externas.
- Su impacto sobre el negocio y las probabilidades de ocurrencia.
- Las medidas correctoras que la organización puede adoptar y su priorización.

La organización está atenta y cuenta con un sistema para recibir información actualizada sobre las amenazas.

La organización cuenta con un análisis de su exposición al riesgo en el área de ciberseguridad en relación con los siguientes parámetros.

- Sector de actividad.
- Ingresos e impacto regional.
- Tipo y cantidad de datos.
- Seguro cibernético solicitado.
- Seguro cibernético previo.
- Eventos IS e historial de pérdidas.
- Marcos y estándares.

La organización identifica y documenta las vulnerabilidades de los activos, recibiendo de foros y fuentes de intercambio de información la inteligencia de amenazas cibernéticas, que son documentadas e identificadas.

Se utilizan las amenazas las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo, estos también se identifican, así como las probabilidades del negocio, priorizando las respuestas al riesgo.

Estrategia de gestión de riesgos

Existe una política de ciberseguridad en la que se incluye de forma explícita y exhaustiva una descripción de las prioridades, restricciones y tolerancia de riesgo específicas de la organización. En base a esta tolerancia al riesgo se deberán tomar las decisiones de riesgos operacionales.

La determinación de esta tolerancia al riesgo tiene en cuenta la posición de la organización en su entorno empresarial. Al determinar la tolerancia al riesgo hay que tener en cuenta aspectos económicos y reputacionales.

Para determinar la tolerancia al riesgo es necesario tener en cuenta si se trata de una infraestructura crítica así como el análisis del riesgo específico del sector económico en el que la empresa esté operando.

En base a la tolerancia al riesgo se deben elegir los tratamientos de riesgo necesarios para alinear el riesgo residual objetivo con el riesgo residual actual, de forma que se puedan priorizar las acciones de tratamiento y las inversiones necesarias para poder alcanzar el nivel de riesgo residual objetivo aprobado.

Los actores de la organización, establecen, gestionan y acuerdan los procesos e la gestión de riesgos, determinando la tolerancia del riesgo de la organización basada en parte en el rol de la infraestructura crítica y el análisis del riesgo específico del sector.

Gestión del riesgo de la cadena de suministro

La identificación, evaluación y gestión de riesgos incluye los riesgos derivados de la cadena de suministro cibernética.

La gestión del riesgo de la organización tiene en cuenta a los proveedores de la organización y los productos, componentes y servicios que cada proveedor facilita.

Para adoptar decisiones relativas a la cadena de suministro se tienen en cuenta las prioridades, limitaciones, tolerancias de riesgo aprobadas por la organización.

Todos los actores de la organización que toman decisiones sobre proveedores, identifican, establecen, evalúan gestionan y acuerdan los procesos de gestión de riesgos sobre la cadena de suministro.

Los contratos con los proveedores establecen las medidas y parámetros de actuación necesarios para que la organización pueda cumplir con sus objetivos de ciberseguridad. En dichos contratos se establecerán asignaciones de riesgos adecuadas, estableciendo penalizaciones o indemnizaciones a los proveedores para el supuesto de que se incumplan las medidas de seguridad o se ocasionen vulnerabilidades o perjuicios para la organización.

Asimismo, se incluirán en los contratos con proveedores y socios externos medidas adecuadas destinadas a garantizar la seguridad cibernética alineadas con el plan de gestión de riesgos de la cadena de suministro cibernético.

En los contratos se exigirá, en la medida de lo posible, que los proveedores de IT y socios externos dispongan de su propia póliza de ciberriesgos, con garantía suficiente como para cubrir las posibles consecuencias que pudiera tener una actuación no conforme durante el cumplimiento de sus obligaciones contractuales.

Los proveedores de IT y socios externos, son evaluados regularmente de forma periódica mediante auditorias, pruebas y otras formas de evaluación, de forma que se compruebe que cumplen con sus obligaciones contractuales. Esta evaluación se tiene en cuenta en la priorización de los proveedores.

Fase 2 Protección

Medidas para proteger los sistemas y evitar que se produzca un incidente.

Medidas

Gobernanza

Existe una política de seguridad documentada, revisada y distribuida

Uno de los principales objetivos del desarrollo de una política de seguridad de la información es gestionar proactivamente el riesgo de sufrir una brecha, ya sea derivada de un fallo de seguridad o de un fallo de sistema, que comprometa y desvele dicha información.

Por tanto, la gestión de la ciberseguridad, esencial para la prevención y protección proactiva de los ciberincidentes, requiere del establecimiento de un marco de gobernanza en el que se definan los responsables de dicha gestión. Dichos responsables serán los encargados de definir y desarrollar las pautas que conformarán la política de seguridad de la información de la organización, documentarla, revisarla y actualizarla periódicamente conforme a las circunstancias, evolución de la actividad/negocio, complejidad creciente del entorno y cumplimiento normativo que se precie a cada momento.

Que la política de seguridad esté distribuida significa que existe una clara voluntad de concienciar e implicar a toda la organización para que todos los empleados, directivos y stakeholders contribuyan a su protección y a la reducción de las posibilidades de un incidente.

Existen políticas de privacidad de información confidencial

Cualquier entidad debe establecer unas políticas proactivas de privacidad de la información, no solo por la obligación de cumplir con la normativa y legislación vigente (RGPD y otras normativas homologas fuera de la UE), sino también por un sentido de la responsabilidad con sus empleados, clientes, usuarios, proveedores y cualquier otro tercero que le ceda o comparta datos personales u otro tipo de información que pudiera ser confidencial (patentes, planes de negocio, etc.).

La información confidencial y de carácter personal es muy sensible y fundamental para una organización y por eso codiciada por parte de los ciberatacantes.

Por otro lado, es esencial que existan políticas de privacidad de dicha información confidencial para que todas las áreas de la organización y usuarios sean conscientes de la forma específica de tratar y almacenar los datos confidenciales. El objetivo de dichas políticas es establecer los procedimientos necesarios para evitar que aquella información confidencial y privada sea tratada de forma indebida.

Los procedimientos deberán ser los más detallados posible, y además de ceñirse a lo establecido en la normativa o legislación pertinente, incluyendo una definición del tipo de información y un registro de la información confidencial y privada para que en caso de ciberincidente se corte o minimice cualquier fuga de datos teniendo en cuenta otras repercusiones como las reputacionales, legales, sanciones, etc.

Existe un CISO y sus responsabilidades están claramente definidas

El CISO (*Chief Information Security Officer*) es el director de seguridad de información y su función principal es la de alinear la seguridad de la información

con los objetivos de negocio para minimizar los riesgos operativos de la organización en caso de incidente.

Cabe destacar que es un cargo de reciente creación (hace 10 años apenas existía este cargo en los organigramas de las entidades) y en muy poco tiempo es una de las figuras que más peso y relevancia está tomando en la mayoría de las organizaciones.

Al CISO le corresponde **liderar** el desarrollo e implementación de las políticas de seguridad de la información y de garantizar la seguridad y privacidad de los datos en todo momento, anticipando nuevas amenazas y trabajando activamente para evitar que ocurran, y si ocurren, que sea capaz de gestionar y mitigar los daños a partir de los planes de respuesta desarrollados, implementados y probados. Además, se encarga de supervisar la administración del control de acceso a la información y el cumplimiento normativo de la seguridad de la información. También es responsable de gestionar y coordinar la respuesta ante los incidentes de seguridad de la información entre todas las personas que formen parte de ese equipo de respuesta.

La existencia de un CISO con responsabilidades claras y definidas garantiza que la información de la organización está protegida adecuadamente en todo momento y, por tanto, es una muestra de que la seguridad de la información es prioritaria para la organización.

Existe un DPO y sus responsabilidades están claramente definidas

El DPO (Data Protection Officer) es una figura que presenta la GDPR (General Data Protection Regulation), cuyas principales funciones son la de supervisar, controlar y coordinar el funcionamiento de esta regulación, o dicho de otro modo, gestionar y supervisar el correcto cumplimiento de la GDPR por parte de la empresa. Es un perfil que debe gozar de independencia a la hora de realizar sus funciones.

Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política

Los archivos generados por la organización deberán seguir lo marcado en la política de seguridad de la información con especial atención a los archivos

confidenciales, de carácter personal y sobre todo de los que comprometan la continuidad del negocio.

Así como también, es importante asegurarse que dichas políticas se ciñen a lo establecido en la normativa y legislación actual ya sea en materia de protección de datos RGPD y otras legislaciones homologas fuera de la UE) y en materia de ciberseguridad (normativa NIS, normativa de pagos electrónicos, etc.)

Los registros de auditoría deben dejar evidencias del cumplimiento de la política.

Los contratos con terceros incluyen requerimientos de ciberseguridad

Trabajamos con información y datos que compartimos, así como también con sistemas electrónicos interrelacionados con terceros ya sean proveedores tecnológicos, la AA.PP, clientes, etc. Esto quiere decir que un incidente de ciberseguridad que afecte a la entidad puede tener su origen en los sistemas de un tercero. Por esa razón es clave revisar los contratos con terceros para que asuman su responsabilidad con las coberturas adecuadas en caso de ciberincidente.

Si es posible, optar por *partners* que prioricen la ciberseguridad, con medidas de seguridad similares a las implementadas por la propia organización especialmente en el caso de proveedores de servicios de IT.

Si para todos es habitual exigir a nuestros socios, *partners*, proveedores y otros terceros, que dispongan de coberturas de Responsabilidad Civil General y Responsabilidad Civil Profesional que garanticen los perjuicios económicos que sus errores y omisiones nos puedan causar, empieza a ser fundamental solicitar también que dispongan de cobertura por los perjuicios económicos que sus fallos de seguridad o de sistemas nos puedan ocasionar.

Al final, poder garantizar un tratamiento adecuado de los datos personales e información confidencial que manejamos no depende única y exclusivamente de la protección de nuestros sistemas electrónicos ni de la implementación de nuestra política de seguridad de la información.

Nuestros sistemas están interrelacionados, por lo tanto, debe exigirse y garantizarse la responsabilidad a esos terceros nombrados en el primer párrafo.

Gestión de la identidad y control de acceso

Los roles y permisos se gestionan según los principios de menor privilegio y separación de actividades

El principio de menor privilegio restringe el acceso del usuario para que solo pueda utilizar las funcionalidades o información que son esenciales para desempeñar su trabajo. Este enfoque permite acotar y minimizar el impacto de un ataque, al tener reducido el usuario el acceso al sistema.

Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados

De poco vale disponer de grandes medidas de protección tecnológicas si no controlamos correctamente que personas o equipos pueden acceder al sistema. La emisión de credenciales, verificación y revocación debe realizarse de acuerdo con unos procedimientos establecidos, que además es auditado para comprobar su aplicación.

Cuentas genéricas: no están permitidas o, si existen están inventariadas y asignadas a un único responsable

Las cuentas para acceder a los sistemas deben ser personalizadas y nunca genéricas. Es necesario que se pueda seguir la traza del usuario concreto que entra en los sistemas de información tanto para detectar posibles incidencias como para conocer como se ha producido un daño y su posible impacto.

Si por cuestiones operativas o hasta que se eliminan estas cuentas es necesario mantenerlas, estas deben ser objeto de especial control, por lo que deben estar inventariadas y asignadas a una única persona, que será la responsable de esta.

Se cancelan todos los accesos y cuentas de usuarios cuando un empleado se da de baja en la empresa

Cuando un usuario causa baja en la empresa deja de tener la necesidad de utilizar los sistemas de información de esta. En consecuencia hay que cancelar de forma sistemática todos los accesos y cuentas de las que disponga.

Una variante de este asunto sería el cambio de funciones de una persona. Se deben cancelar los privilegios que tuviese en su antiguo puesto y asignarle los nuevos.

Se gestiona el acceso remoto

Es más fácil proteger un entorno interno que uno externo. Por eso es necesario aumentar las medidas de seguridad cuando se accede desde fuera de la organización.

El acceso remoto está restringido a las redes privadas virtuales (VPN)

Una medida para reforzar la seguridad cuando se accede desde el exterior es utilizar redes VPN.

Estas son un método utilizado para conectarse a internet de forma privada. Para conseguirlo el sistema oculta la dirección IP real (la 'matrícula' que identifica un equipo en la red) y enruta tanto el tráfico como los datos a través de un túnel privado y cifrado de forma segura a través de redes públicas.

Se aplica autenticación multifactor a todas las conexiones remotas

La autenticación multifactor o MFA es un método de control de acceso informático en el que es necesario que el usuario presente dos o más pruebas para garantizar quién es. A la tradicional contraseña se añade una clave segunda rotatoria (recibida por ejemplo a través de un móvil registrado), un certificado digital instalado en el equipo, biometría, etc.

Línea Roja Mercado Asegurador: Sin el uso de MFA en todas las conexiones remotas será muy complicado obtener una cobertura aseguradora razonable.

Esta será probablemente la medida más importante de entre todas las que se señalan en este documento.

Se gestiona y se protege el acceso físico a los activos

La seguridad de acceso físico evita que las personas entren en contacto directo con los componentes informáticos. Los controles técnicos no pueden eliminar todos los daños, por lo que hay que controlar también la seguridad física de los activos para evitar situaciones como el robo, el daño o el acceso directo a los equipos, sistemas de almacenamiento, etc.

Separación de las cuentas de administración para estaciones de trabajo, servidores y controladores de dominio

Un controlador de dominio restringe el acceso a los recursos de un dominio autentificando la identidad del usuario mediante credenciales de inicio de sesión. El controlador de dominio media los accesos a la red.

La segregación de las cuentas de administración (la misma persona tiene cuentas distintas para las distintas funciones que realiza) permitirá limitar los daños que pueden producirse en los sistemas si un tercero consigue sus credenciales.

Línea Roja Mercado Asegurador: La segregación de cuentas de administración para estaciones de trabajo, servidores y controladores de dominio es algo muy importante para los equipos de suscripción.

Los administradores tienen una credencial única y privilegiada

Los administradores del sistema tienen los mayores privilegios de acceso al sistema. Serán por tanto las cuentas más codiciadas por los cibercriminales en tanto que se trata de las cuentas con las que mayor daño pueden producir y requieren una política de seguridad más estricta.

Para desempeñar tareas comunes, al administrador debe disponer de un usuario diferente del que utiliza cuando tiene que realizar funciones de administración del sistema.

Las cuentas privilegiadas (incluidas las cuentas de servicio con privilegios de administrador) requieren autenticación multifactor

Cuanto mayor sea el número de elementos que tenga que utilizar para acceder a un sistema, más difícil resultará suplantar la identidad de una persona. Para las cuentas privilegiadas debe implantarse una autenticación con varios componentes.

Línea Roja Mercado Asegurador: Las cuentas privilegiadas, incluidas las cuentas de servicio con privilegios de administrador que deberían ser eliminadas en su totalidad o reducidas lo máximo posible, deben contar con MFA así como medidas adicionales y específicas de protección.

Existe un registro de las acciones realizadas desde cuentas privilegiadas

Estas cuentas deben estar sujetas a un seguimiento especial. Debe quedar un registro detallado de todas las acciones privilegiadas, de forma que se permita detectar patrones de comportamiento irregulares que puedan anticipar un posible incidente o en caso de un incidente, facilitar el análisis para determinar el alcance de los daños.

Concienciación y capacitación

Todos los usuarios están informados y capacitados.

Las personas son una pieza clave en la ciberseguridad y todos los usuarios forman parte de la estrategia de seguridad de la empresa. Los diferentes ciberataques se producen en numerosas ocasiones por fallos de empleados.

Los usuarios deben conocer los elementos claves de seguridad y estar capacitados para identificar y evitar un ciberataque y ataques de ingeniería social.

Los programas de concienciación incluyen al menos: e-learnings, campañas de phising, ejercicios de gestión de crisis, alertas de email…

Los programas de concienciación deben tratar de concienciar dinámicamente las áreas de la empresa creando programas distintos para cada una

de ellas. Esto permitiría generar mayor interés e implicación del empleado en el programa de concienciación, aumentando eficacia y eficiencia del proceso.

Los programas de concienciación están adaptados a las diferentes necesidades de los usuarios y son de asistencia obligatoria

El riesgo de un ciberataque está siempre en aumento y constantemente surgen nuevas amenazas lo que exige que los programas de concienciación sean continuos y para todos los usuarios, al menos, con carácter anual y a toda la organización.

Datos

Se protegen los datos en reposo y en tránsito para verificar la integridad de la información

Los datos almacenados y transmitidos se deben proteger y verificar su integridad para garantizar que solo se hayan hecho cambios aprobados.

Los datos (en reposo y en tránsito) se encriptan según su criticidad

Los datos de una empresa se definen su grado de criticidad, siendo los de mayor criticidad aquellos datos que incluyan datos personales, financieros y de salud.

Si una empresa almacena o transmite este tipo de datos sensibles, debe asegurar que sean protegidos por cifrado tanto cuando sean almacenados en computadores como cuando sean transmitidos a otras partes.

Se implementan protecciones contra las filtraciones de datos

Es esencial mantener la privacidad de los datos de una empresa y para ello se implementan distintas medidas de protección, como son: cifrar los datos, mantener contraseñas fuertes/complejas, mantener los sistemas

actualizados correctamente, antivirus, firewall, formación y capacitación de empleado… entre otras.

Los datos son eliminados de acuerdo con las políticas

Se deben eliminar y/o destruir datos de manera segura cuando ya no sean necesarios o requeridos para fines de cumplimiento y de acuerdo con la política de seguridad de la empresa.

Se realizan, se mantienen y se prueban copias de seguridad de la información

Se deben realizar copias de seguridad con regularidad, mantener durante un periodo de tiempo (recomendado 90 días para evitar los efectos de *hackers* que están en la red antes de atacar) y realizar pruebas de reinstalación de estas copias.

Muchos sistemas operativos tienen capacidades integradas para hacer respaldos, también existen soluciones de software y en la nube disponibles que pueden automatizar el proceso de respaldos.

Una buena práctica es mantener un conjunto de datos respaldados fuera de línea con frecuencia para protegerlo contra posibles ataques.

Línea Roja Mercado Asegurador: Se deberán realizar, mantener y probar las copias de seguridad de la organización. Además, la organización deberá contar con copias de seguridad offline con una protección adecuada.

Equipos

Los equipos y los sistemas están protegidos frente a amenazas específicas (Ramsonware, virus, malware, brechas, etc…)

Es necesario conocer cuáles son las principales amenazas y vulnerabilidades a las que nos podemos enfrentar, con el fin de tomar las medidas necesarias que se ajusten a cada amenaza o vulnerabilidad de manera específi-

ca, intentado evitar las generalidades. Algunas de las principales amenazas y vulnerabilidades pueden ser:

- Amenazas de *Malware* (Virus, gusanos, troyanos, *ramsomware*, etc.).
- Vulnerabilidades del sistema (Errores de configuración, en la gestión de recursos, en los sistemas de validación, errores que permiten el acceso a directorios, errores en la gestión y asignación de permisos, etc.).
- Amenazas de ataques de denegación de servicio.
- Vulnerabilidades producidas por contraseñas poco seguras.
- Vulnerabilidades producidas por usuarios (Mala asignación de privilegios, falta de formación que generan otras vulnerabilidades, como la apertura de ficheros de dudosa procedencia, engaños por publicidad falsa, apertura de correos fraudulentos, etc.).

Los equipos portátiles utilizan cifrado de disco completo

El cifrado de disco completo es una tecnología que cifra los datos almacenados en todo el disco duro y no solo de un segmento. Proporciona una protección básica cuando la computadora está apagada, ya que, en el momento en que se apaga, todos sus datos quedan bloqueados. Cualquier persona que intente acceder al disco duro, debe utilizar la contraseña para descifrar los datos.

El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas

Dado que estas tareas pueden ser realizadas por varias personas, es importante tener un registro de todas las actuaciones que se realizan, tanto de mantenimiento como de reparación. Ello nos permitirá tener un mejor seguimiento de los activos y mejorar la seguridad de los equipos.

Las herramientas o programas que se utilicen para estos controles deberían ser aprobados y controlados siguiendo las directrices marcadas en las políticas de seguridad de la empresa.

El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado

Durante los trabajos de mantenimiento en remoto, se intercambia información sensible y se hace accesible a terceros. Por lo tanto, debemos ser capaces, a través de programas de específicos, de garantizar que la conexión es segura y que la persona a la que se concede el acceso es identificable, dejando registro de todo ello.

Se utiliza antivirus en todos los sistemas informáticos (incluidos móviles, tablets, etc…)

Es importante contar con un antivirus en todos los sistemas de la organización y tenerlos actualizados, ya que es nuestra primera línea de defensa. Es muy importante incluir, dentro de esta protección, los móviles, *tablets* o cualquier otro dispositivo que sea utilizado por los usuarios.

Las workstations de acceso privilegiado (no tienen acceso a internet o email) se utilizan para la administración de sistemas críticos

Los sistemas críticos de la organización deben ser especialmente protegidos y su administración debe ser realizada por usuarios con la configuración de seguridad más alta, con el evitar que su información de acceso pueda ser vulnerada o robada por personas ajenas a la organización. No obstante, el acceso a los sistemas críticos debe ser monitoreado y controlado en todo momento.

Utilizando accesos privilegiados sin acceso a internet o email conseguiremos mantener aislados los sistemas críticos de la red de internet, ofreciéndole así una mayor seguridad.

Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición

Estos procesos pueden suponer un riesgo para la seguridad de los datos. Debemos ser capaces de proteger la confidencialidad, integridad y disponibili-

dad de la información contenida en los equipos. Para ello, las personas responsables de estas gestiones, deben tener claro los procedimientos a utilizar en casa caso.

Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política

Los riesgos principales de los medios extraíbles son: la pérdida o robo, el acceso a la información o la infección por malware. Por ello, estos dispositivos deben contar con la protección adecuada y su uso debería quedar regulado siguiendo las políticas de empresa.

Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware

Es importante verificar que ninguno de los componentes físicos del sistema ha sido modificado. Sería necesario disponer de la infraestructura necesaria que nos permita valorar la seguridad e integridad de toda los equipos o sistemas de la organización.

Aplicaciones

La seguridad de las aplicaciones está garantizada utilizando mecanismos de protección frente a amenazas específicas. Ejem: SQL-injection, Cross-site scripting, Spam, Data breach, vulnerabilidad de día 0

Se deben usar todos los mecanismos disponibles para prevenir los ataques:

SQL-injection es una técnica de inyección de código que podría destruir su base de datos. La inyección SQL es una de las técnicas de piratería web más comunes.

La única forma segura de prevenir los ataques de inyección SQL es la validación de entrada y las consultas parametrizadas, incluidas las declaraciones preparadas. El código de la aplicación nunca debe usar la entrada directamente. El desarrollador debe desinfectar todas las entradas, no solo las entradas de formularios web, como los formularios de inicio de sesión.

Cross-site scripting (también conocido como XSS) es una vulnerabilidad de seguridad web que permite a un atacante comprometer las interacciones que los usuarios tienen con una aplicación vulnerable. Permite a un atacante eludir la misma política de origen, que está diseñada para segregar diferentes sitios web entre sí. Las vulnerabilidades de secuencias de comandos entre sitios normalmente permiten que un atacante se haga pasar por un usuario víctima, lleve a cabo cualquier acción que el usuario pueda realizar y acceda a cualquiera de los datos del usuario. Si el usuario de la víctima tiene acceso privilegiado dentro de la aplicación, entonces el atacante podría obtener control total sobre toda la funcionalidad y los datos de la aplicación.

La prevención de secuencias de comandos entre sitios es trivial en algunos casos, pero puede ser mucho más difícil según la complejidad de la aplicación y la forma en que maneja los datos controlables por el usuario.
En general, es probable que la prevención eficaz de las vulnerabilidades XSS implique una combinación de las siguientes medidas:

- Entrada de filtro a la llegada. En el punto donde se recibe la entrada del usuario, filtre lo más estrictamente posible en función de lo que se espera o de la entrada válida.
- Codificar datos en la salida. En el punto donde los datos controlables por el usuario se emiten en las respuestas HTTP, codifique la salida para evitar que se interprete como contenido activo.
- Use encabezados de respuesta apropiados.
- Política de seguridad de contenido. Como última línea de defensa, puede usar la Política de seguridad de contenido (CSP) para reducir la gravedad de las vulnerabilidades XSS que aún ocurren.

Spam es un mensaje de email no solicitado que se envía automáticamente a un gran número de direcciones al mismo tiempo. Comúnmente llamado correo basura, el spam se usa con mayor frecuencia para fines de *marketing*, aunque los *hackers* pueden usarlo también para repartir malware. Se deben introducir mecanismos para evitar su entrada como el antispam que se conoce como "método para prevenir el correo basura". Tanto los usuarios finales como los proveedores de servicios de correo electrónico utilizan diversas técnicas contra ello.

Data breach o brecha de seguridad, debemos asegurarnos de que los datos estén adecuadamente protegidos para evitar pérdidas o robos de datos.

Vulnerabilidad de día cero o *Zero Day* es una vulnerabilidad de software que los atacantes descubrieron antes de que el proveedor sepa siquiera de su existencia, por lo que aún no existen parches.

El ciclo de desarrollo de sistemas / software (system development life cycle) está implementado y los requisitos de seguridad se incluyen según los principios de privacidad por diseño / por defecto

El ciclo de vida de desarrollo de sistemas (SDLC) es un modelo conceptual utilizado en la gestión de proyectos que describe las etapas involucradas en un proyecto de desarrollo de sistemas de información, desde un estudio de viabilidad inicial hasta el mantenimiento de la aplicación completa. SDLC puede aplicarse a sistemas técnicos y no técnicos. Este modelo tiene integrada la privacidad.

Se utilizan procedimientos para prevenir cambios no autorizados e instalar proactivamente las actualizaciones de seguridad

Ello redunda en evitar posibles ataques y modificaciones que puedan producir que no accedamos a los datos, se encripten...

Se deben instalar las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores y programas antivirus.

Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información

Los mecanismos de seguridad son herramientas técnicas y métodos técnicos que se utilizan para implementar los servicios de seguridad. Un mecanismo puede funcionar por sí solo, o con otros, para proporcionar un servicio determinado. Los mecanismos básicos de seguridad son:

- Autenticación.
- Autorización.

- Administración.
- Auditoría y Registro.
- Mantenimiento de la Integridad de la información.

Existe un proceso de parcheado frecuente

Se deben de establecer un proceso de parcheado frecuente del *software* con el fin de evitar los ataques dirigidos a las vulnerabilidades descubiertas por el desarrollador del *software* y que por tanto son conocidas por los *hackers*.

Línea Roja Mercado Asegurador: Para cumplir con los estándares del mercado, el equipo de ciberseguridad debe buscar activamente posibles vulnerabilidades de *software* y parchear frecuentemente.

Redes

Una red de comunicación es un conjunto de medios técnicos (hardware y software) que permiten la comunicación remota entre dispositivos independientes.

Las redes de comunicaciones y control están protegidas. Se protege la integridad de la red

La protección de redes pretende evitar que personas no autorizadas se introduzcan en el sistema, evitar que los usuarios realicen operaciones que puedan dañar al sistema (p.ej. limitando el acceso a internet), garantizar que no se interrumpa el servicio…

La integridad es la propiedad que busca mantener la red libre de modificaciones no autorizadas. Es mantener con exactitud la red tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

Las siguientes medidas ayudan a proteger las redes: mantenimiento rutinario de equipos, antivirus, *firewalls*, uso de contraseñas robustas, encriptación a través de una VPN (*Virtual Private Network*), segmentación de la red, etc.

Las redes están aisladas de los sistemas de control industrial (SCADA, PLC, DPC…)

Una red aislada es una red que está físicamente aislada de cualquier otra red para aumentar su seguridad. Los equipos que constituyen esa red no pueden comunicarse ni trabajar con los equipos de otras redes. Al estar aisladas, aumenta el nivel de protección. No tendría acceso por internet ni tampoco desde otras redes de la misma organización.

Los sistemas de control industrial (OT Operation Tecnology) tienen como finalidad controlar y gestionar de la manera más eficiente los distintos procesos industriales. Dentro de estos sistemas encontramos SCADA (*Supervisory Control and Data Adquisition*), PLC (*Programmable Logic Controller*) y DPC (*Discrete Process Control*).

Segmentación de la red: por geografía, por funciones de negocio, etc.

La segmentación de red es una técnica de seguridad que divide una red en distintas subredes, que permiten a los equipos de la red compartimentar las subredes y otorgar controles y servicios de seguridad únicos para cada subred.

Este proceso implica dividir una red física en diferentes subredes lógicas. Una vez dividida en unidades más pequeñas y manejables, se aplican controles a cada segmento individual.

La segmentación puede realizarse con distintos criterios: geográfico, por funciones de negocio, etc.

Línea Roja Mercado Asegurador: Una segmentación de sistemas por geografías y unidades de negocio es un punto básico para poder conseguir una póliza con garantías adecuadas.

La seguridad de la red está garantizada mediante el uso de mecanismos para defenderla de amenazas específicas de red (DoS-DDoS, spam, botnets…)

Existen múltiples mecanismos para garantizar la seguridad de la red. Muchos de estos están diseñados para defenderla de amenazas específicas.

Para ataques de denegación de servicio (DoS-DDoS) se monitoriza el tráfico de información y detectan anomalías. Cuando esta se corresponde con una actividad maliciosa, se redirige el tráfico a un sistema de filtrado (habitualmente basado en la nube) antes de cruzar el borde de la red, trasladando a esta solo el tráfico legítimo para que la actividad de la empresa continúe de la forma habitual.

Para amenazas de spam se utilizan programas antispam.

Para evitar formar parte de una red de botnets se utilizan las medidas habituales para protegerse del malware: cortafuegos, tener el sistema correctamente actualizado, utilizar contraseñas robustas, antivirus, etc.

Se utiliza firewall

Un *firewall* es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Constituye una primera línea de defensa de la seguridad de la red. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza.

Sistemas

Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas

El ciclo de vida del desarrollo de un sistema abarca la vida completa de este, desde que se definen sus requisitos hasta la finalización de su uso.

Para ofrecer una buena experiencia al usuario, eficiencia, seguridad y fiabilidad de uso, es necesario que esté soportado por una metodología. Esta suele contener las fases de planificación, definición de requisitos, diseño, desarrollo y pruebas, implantación o puesta en marcha, mantenimiento y retirada de funcionamiento.

Existe un plan específico para los casos de migración de sistemas IT. Se implementan medidas especiales de seguridad

Un plan de migración de sistemas es el proceso mediante el que realizamos una transferencia de un sistema de información a otro. Se lleva a cabo para reemplazar máquinas o aplicaciones y puede implicar un cambio en los formatos de los datos.

Teniendo en cuenta la importancia de los datos y de los sistemas para el correcto funcionamiento de una organización, la migración es un proceso crítico que debe abordarse de forma planificada y con metodología.

Durante los procesos transitorios pueden producirse unas mayores vulnerabilidades que deben acompañarse de medidas especiales de seguridad.

Se desarrolla y se implementa un plan de gestión de las vulnerabilidades

La gestión de vulnerabilidades es el proceso de identificación, análisis, clasificación y tratamiento de los riesgos derivados de los sistemas, de modo que se puedan corregir las debilidades, aplicar controles y minimizar los impactos negativos.

Los entornos de desarrollo y pruebas están separados del entorno de producción

Los entornos de desarrollo y pruebas deben estar separados del entorno de producción para reducir los riesgos de acceso por personal no autorizado y para evitar problemas operacionales derivados de que cambios que se realizan en entornos de desarrollo/pruebas puedan afectar al sistema en producción.

Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales

Cada persona debe tener exclusivamente acceso a las funcionalidades que necesita para desempeñar el trabajo que tiene designado.

Este planteamiento es esencial para reducir la superficie de ataque y en consecuencia el riesgo de la empresa.

Se encuentran establecidos procesos de control de cambio de la configuración

El control de cambios de configuración es un proceso para controlar, aprobar y hacer un seguimiento de los cambios de configuración. Implica una serie revisiones y aprobaciones por parte de supervisores, técnicos y otras partes interesadas para reducir los riesgos de fallos derivados de los cambios.

Existen controles específicos para los sistemas de información de los proveedores

Es inusual que una empresa no tenga subcontratado algún servicio. Tener bien protegidos/controlados los sistemas propios y no prestar atención a los de los proveedores es un riesgo importante para las organizaciones. Para evitarlos/reducirlos deben solicitarse el cumplimiento de medidas de seguridad y controlar que estas se cumplen.

Otros

Se utiliza un directorio activo (Active Directory)

Un Directorio Activo es una base de datos y un conjunto de servicios que conectan a los usuarios con los recursos de red que necesitan para realizar su trabajo. Esta base de datos contiene información sobre los usuarios y equipos que hay en el sistema y que pueden hacer.

Su objetivo es administrar los inicios de sesión conectados a una red, así como la administración de las políticas de la red. Permite aplicar actualizaciones críticas a una organización entera.

La seguridad física de los edificios está implementada según los mismos principios de riesgo y controles de autenticación del edificio

Aunque los sistemas de información son algo que pueden considerarse intangibles, estos se encuentran soportados por sistemas físicos que se ubican en edificios. La seguridad física es necesaria para la seguridad de los sistemas de información.

Fase 3 Detección

Esta fase tiene como objetivo definir las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad, permitiendo el descubrimiento oportuno de los mismos.La detección de un "ciber act" en una fase temprana es fundamental a la hora de minimizar los posibles daños y tiempos de disrupción de la actividad. Esto nos permitirá reducir el posible impacto a la cobertura de pérdida de beneficios de nuestra póliza ciber así como los gastos asociados a la restitución a la normalidad de los sistemas informáticos (forensics…) lo cual interesa tanto al Asegurado como al Asegurador.

El objetivo de la detección debe ser tomar medidas intencionales para detectar actividades maliciosas antes de que puedan causar un daño en lugar de enfocarse en medidas reactivas una vez tiene lugar la amenaza.

Las principales medidas en esta fase de detección son técnicas, pues resulta imprescindible contar con una continua monitorización de los sistemas que permita detectar cualquier entrada sospechosa. Sin embargo, también podemos encontrar medidas legales y organizativas.

Medidas

Anomalias y eventos

Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas

Es importante que la empresa tenga una base de datos o inventario de operaciones y flujos de datos que se esperan de usuarios y sistemas, para poder localizar las posibles anomalías que ocurran.

Se analizan los eventos detectados

Ya sea internamente o con la ayuda de especialistas externos, la compañía debe analizar los eventos que se hayan podido detectar. Este análisis debe ser llevado a cabo con rapidez y requiere gran capacidad técnica ya que las anomalías pueden ser muy numerosas.

Los datos de los eventos se recopilan y se correlacionan a través de múltiples fuentes y sensores

Como en toda función, es importante obtener información de las ocurrencias. Será conveniente recopilar todos los eventos que ocurran y con software adecuado buscar tendencias, que puedan permitir anticipar futuros incidentes.

Se determina el impacto de los eventos

Como continuación del punto anterior, los eventos se podrán valorar, siguiendo el criterio habitual en Seguros, para buscar la máxima perdida posible (*Estimated Maximum Loss, EML*) por un lado y el impacto agregado de todos los eventos, teniendo en cuenta el efecto económico directo del evento, y otros efectos indirectos de interrupción de negocio o más allá como daños reputacionales o de imagen.

Se establecen umbrales de alerta de incidentes

De nuevo al igual que en Seguros, se debe establecer un umbral o si queremos llamarlo "franquicia" en los eventos, de manera que se pueda optimizar los recursos de la compañía al hacer frente a los mismos.

Vigilancia continua de la seguridad

Se monitorea la red

Mediante un análisis pormenorizado del tráfico de red analizando no solo el tipo de tráfico sino también el contenido y su comportamiento.

Línea Roja Mercado Asegurador: La monitorización de la actividad de la red de la empresa mediante herramientas como los sistemas SOC o SIEM será clave para los equipos de suscripción de las aseguradoras. En caso de no contar con estos sistemas se deberá justificar por qué no se cuenta con ellos y describir las medidas alternativas de monitorización implementadas.

Se monitorea el entorno físico

Se trata de evitar el acceso físico de intrusos tanto a Áreas Seguras (instalaciones de procesamiento de información y la información de la organización), como a Equipamiento previendo pérdidas, daños, hurtos… de los activos.

Se monitorea la actividad del personal

Como parte del monitoreo de toda la actividad de la empresa en la red, debe tenerse en cuenta aquella generada por los propios empleados de la organización. Es un tema controvertido debido a la invasión de la privacidad del personal que puede implicar. El personal debe ser informado sobre las medidas adoptadas por la organización para monitorizar su actividad.

Se detecta el código malicioso

El código malicioso o "*malware*" es un software que un cibercriminal o hacker ha creado para interrumpir o dañar el equipo de un usuario legítimo. Con frecuencia propagado a través de un archivo adjunto de correo electrónico no solicitado o de una descarga de apariencia legítima, el malware puede ser utilizado por los ciberdelincuentes para ganar dinero o para realizar ciberataques con fines políticos.

Hay diferentes tipos de *malware*, entre los que se incluyen los siguientes:

- Virus: un programa capaz de reproducirse, que se incrusta un archivo limpio y se extiende por todo el sistema informático e infecta a los archivos con código malicioso.
- Troyanos: un tipo de *malware* que se disfraza como *software* legítimo. Los cibercriminales engañan a los usuarios para que carguen troyanos a sus computadoras, donde causan daños o recopilan datos.
- *Spyware*: un programa que registra en secreto lo que hace un usuario para que los cibercriminales puedan hacer uso de esta información. Por ejemplo, el *spyware* podría capturar los detalles de las tarjetas de crédito.
- *Ransomware*: *malware* que bloquea los archivos y datos de un usuario, con la amenaza de borrarlos, a menos que se pague un rescate.
- *Adware*: *software* de publicidad que puede utilizarse para difundir *malware*.
- *Botnets*: redes de computadoras con infección de *malware* que los cibercriminales utilizan para realizar tareas en línea sin el permiso del usuario.

Su detección temprana y neutralización es fundamental.

Se detecta el código móvil no autorizado

Se refiere al código utilizado por desarrolladores web para incorporar funcionalidades y mejorar la apariencia de las páginas web. Puede incluir algún "*malware*" con lo que deber ser también monitorizado.

Se monitorea la actividad de proveedores de servicios externos

Debido a la externalización de servicios dentro de los sistemas de la información de las organizaciones, un "*ciber act*" sufrido por uno de sus proveedores puede extenderse a los sistemas del cliente. Debido a esto, es fundamental detectar cuanto antes cualquier evento que pueda haber sufrido uno de nuestros proveedores de forma que se puedan cortar los puentes que unan nuestros sistemas con los del proveedor a la mayor brevedad. De esta forma la organización sufrirá los efectos de no disponer de los servicios proporcionados por el proveedor, pero evitará que sus propios sistemas se vean comprometidos.

Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados

Es fundamental que una organización disponga de una política de ciberseguridad en la que se establezcan los distintos tipos de usuarios, quién puede acceder a qué información, cuál es la forma segura de acceder a los sistemas corporativos, qué dispositivos se pueden usar para desarrollar la actividad profesional y cómo se maneja el uso y actualización de los distintos *softwares* autorizados.

Se realizan escaneos de vulnerabilidades

Se trata de buscar los puntos débiles en materia de ciberseguridad de un sistema informático ya sea en la red o en aplicaciones web como cortafuegos, impresoras, *routers*, servidores web, sistemas operativos, vulnerabilidades en la nube, componentes de herramientas de código abierto, testeo de seguridad de aplicaciones.

Procesos de detección

Los roles, las actividades y los deberes de detección están bien definidos

Los procesos de detección dependen, en la mayor parte de las organizaciones, de equipos transversales que incluyen personas o equipos de diferentes ámbitos, desde la ciberseguridad hasta la tesorería. Cada una de estas piezas debe conocer en detalle que sección de detección le corresponde y ante qué tipo de ataques debe estar alerta.

Las actividades de detección cumplen con todos los requisitos aplicables

Las actividades de detección deben ser amplias, y cubrir tanto el interior de la empresa como el exterior. El entorno digital es una fuente de información tan valiosa como los análisis de sistemas internos.

Deben ser continuas, y buscar de forma ininterrumpida variaciones o anomalías en las redes, como tráficos o consumos de recursos inusualmente altos, incrementos de conexiones detenidas por el cortafuegos, llegadas masivas de correo basura, o problemas de conexión en los dispositivos móviles.

Deben ser consistentes, analizando los diferentes repositorios en los que se encuentra una misma información.

Deben ser completas, ya que cualquier brecha puede ser utilizada por los ciberdelincuentes para introducir una amenaza.

Se prueban los procesos de detección

Estos procesos deben ser puestos a prueba de forma interna para buscar debilidades en su entramado. Las pruebas pueden ser tanto internas, utilizando auditores de la organización, como externas, haciendo uso de empresas especializadas en detección de ciberincidentes.

Se comunica la información de la detección de eventos

Una vez detectado el evento se debe iniciar la solución o bloqueo del mismo. Para ello es necesario que los canales de comunicación de eventos sean efectivos y trasladen la información desde el foco de detección al CISO de la organización que puede activar el proceso de supresión del incidente.

Los procesos de detección se mejoran continuamente

Se debe asegurar que estos procesos cumplen las mejores prácticas del mercado y están actualizados. El mundo cibernético se encuentra en continua evolución, lo que genera de forma ininterrumpida nuevas áreas de vulnerabilidad que deben ser incluidas en los procesos de detección.

Fase 4 Respuesta

Objetivo: Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de seguridad cibernética.

Medidas

Planificación de respuesta

Realiza simulacros periódicos de escenarios de incidentes

Los escenarios de incidentes son documentos que recogen escenarios probables y sus impactos sobre la organización.

Realizar simulacros en los que se pone a prueba la respuesta de la empresa a estos eventos reduce el tiempo de actuación y prepara a los equipos para casos reales.

Dispone de un plan de auditoría/hacking ético sobre las principales aplicaciones e infraestructuras

Las auditorias o hackings éticos son situaciones reales en las que expertos en ciberdelincuencia realizan ataques sobre la organización. Dependiendo del ni-

vel de madurez de los sistemas de ciberseguridad es posible que los ataques precisen generar internamente una vulnerabilidad en las redes.

El someter a los sistemas a este tipo de ataques nos permite confirmar la robustez de las protecciones de la organización y detectar posibles vulnerabilidades de forma preventiva.

Dispone de una política de seguridad de la información

Consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que la afectan.

Con una buena política de seguridad de la información (realizar copias de seguridad, utilizar contraseñas fuertes, proteger el contenido de las claves…) conseguimos minimizar los riesgos que la afectan.

Dispone de un Comité de Gestión de Crisis, sujeto a revisión periódica

El Comité de Crisis es una figura táctica y de decisión clave en la gestión de cualquier situación crítica. Su objetivo es múltiple: Tiene que asumir la responsabilidad de la comunicación de crisis, estudiar el problema, valorar la gravedad del mismo, aliviar en lo posible los daños, tomar decisiones, etc.

Cualquier organización es candidata a padecer un ataque, por lo que el crear este comité antes de la ocurrencia del evento, y entrenarlo con simulacros periódicos es clave para una buena gestión del incidente.

Dispone de BCP sujeto a revisión periódica

Un Plan de Continuidad de negocio (BCP) es un documento que consta de la información crítica que necesita una empresa para continuar operando durante un evento no planificado. El BCP debe establecer las funciones esenciales de la empresa, identificar qué sistemas y procesos deben mantenerse y detallar cómo mantenerlos.

Contar con un BCP ayudará a identificar rápidamente los procesos críticos en caso de incidente y acelerará de esta forma la recuperación de la actividad.

Dispone de un servicio de soporte 24/7 para las aplicaciones críticas

Los servicios de soporte especializados son claves en la recuperación de los equipos. Si contamos con servicios 24/7 capaces de responder rápidamente en caso de incidente minimizaremos los tiempos de recuperación de la actividad de la empresa. Estos servicios deberían priorizar las aplicaciones críticas para una mayor efectividad.

Dispone de un DRP actualizado

El Plan de Recuperación de Desastres (DRP) describe cómo una empresa puede reanudar el trabajo rápidamente después de un incidente. Un DRP tiene el objetivo de apoyar a una organización a resolver la pérdida de datos y recuperar la operatividad de un sistema luego de un incidente no planeado. Además, forma parte del BCP.

Al igual que el BCP, el DRP es importante para agilizar la recuperación de la actividad tras un incidente pero se diferencia del anterior en que está específicamente relacionado con el área de IT y se refiere a las acciones que se van a emprender para resolver cualquier eventualidad que impida que el personal acceda al sistema.

Además, este plan establece el tiempo objetivo de recuperación (RTO), que es el periodo máximo que puede tardar el negocio en reanudar operaciones; y el punto objetivo de recuperación (RPO), es decir, el punto máximo de datos que se pueden perder en el evento sin comprometer el resto de la información.

Revisar que como medida de protección existe copias de seguridad en sitios diferentes (copias físicas), no todas pueden ser holísticas (no todas completas y a tiempo real) para información crítica.

Realiza análisis de AV/EDR

Las herramientas de "*Endpoint Detection and Response*" (EDR) son herramientas que proporcionan monitorización y análisis continuo de los "*endpoints*" y la red. Su finalidad es detectar y prevenir amenazas de forma automática.

Este tipo de sistemas instalados en la red realizarán análisis de forma continua para detectar anomalías en la red y nos alarmará rápidamente en caso de que se esté produciendo un ataque o se detecte una amenaza. De esta forma se reducen drásticamente los tiempos de detección de incidentes.

Línea Roja Mercado Asegurador: Contar con una herramienta EDR (o versiones superiores) será necesario si queremos contar con una buena cobertura aseguradora.

Realiza ejercicios de Threat Hunting

Son procesos de búsqueda iterativa y proactiva a través de las redes para detectar y aislar amenazas avanzadas capaces de evadir las soluciones de seguridad existentes.

Son herramientas cuya clave es la proactividad con la que actúan, ya que permiten a la organización conocer las posibles amenazas y adelantarse a ellas, haciendo que su detección sea lo más rápida posible.

La realizan equipos de seguridad *red* (expertos en atacar sistemas) y *blue* (profesionales en mantener las defensas de la red interna).

Comunicaciones

Existencia de campañas periódicas de sensibilización a los empleados, que incluya capacitación sobre las prácticas a seguir tras la activación de una crisis con el objetivo de mitigarlo

Las campañas periódicas de sensibilización a los empleados **permiten conocer el rol de los empleados y el orden de las operaciones** necesarias para dar respuesta a una crisis.

Estas campañas **permiten** que las partes interesadas tenga una **mayor conciencia** de la ciberseguridad en la empresa, así como un conocimiento de los riesgos que permite **desarrollar actuaciones para mitigarlo.**

Existencia de un plan de activación de crisis a los miembros de comité de gestión de crisis que incluya varios canales de localización (teléfono, email, whatsapp, etc.)

El plan de activación de crisis se ejecuta durante y después de un incidente según los criterios establecidos en el plan de respuesta y facilita la coordinación de las partes interesadas.

El plan de comunicación de crisis **establece:**

- los **criterios** del plan.
- los **roles** que deben asumir los empleados.
- el **orden** de las operaciones a realizar.

Es necesario que el plan este **actualizado y sea probado**. Probar los planes de respuesta permite asegurarse que cada persona conoce sus responsabilidades al ejecutar el plan. Cuanto más preparada este una organización la respuesta será más efectiva, esto incluye el intercambio entre las partes interesadas y los reportes legales.

Probar el plan (y la ejecución durante un incidente) permitirá desarrollar las mejoras necesarias a incluir en su actualización. Es conveniente que los planes de respuesta **incluyan las lecciones aprendidas.**

El plan de comunicación debe incluir a todos los proveedores externos y a las partes interesadas clave. Los proveedores pueden contribuir a su mejora, tanto en el planteamiento como en la ejecución.

En el caso de un evento de seguridad, la empresa debe trabajar rápidamente y exhaustivamente para comprender la amplitud y profundidad del impacto de este evento, buscar ayuda, **comunicar la información de la situación a las partes interesadas** (incluyendo los clientes) y mejorar políticas y procedimientos de ciberseguridad que permitan evitar o mitigar los efectos.

Existencia de un plan de comunicación de crisis a las autoridades (escalado a las autoridades de privacidad, supervisor y autoridades tecnológicas) y medios de comunicación que incluya un argumentario reactivo y un Q&A

La respuesta ante una crisis de ciberseguridad incluye requerimientos de reportes legales e intercambio de información con las autoridades.

Ante un evento de seguridad, la comunicación del mismo es clave para la empresa tanto por proteger su reputación como porque el hecho de liderar la comunicación evita mensajes confusos o erróneos.

Análisis

Realiza análisis para garantizar una respuesta eficaz y apoyar las actividades de recuperación

El análisis del incidente es una parte fundamental del proceso de gestión de un evento cibernético. Para poder actuar de forma efectiva es necesario evaluar mediante análisis el alcance y el impacto que el incidente supone. La aseguradora ofrece la posibilidad de realizar el análisis y/o apoyar al asegurado en este análisis.

Dependiendo del resultado del análisis las medidas de actuación serán mayores o menores, o implicarán o no a partes de la organización que típicamente no se ven afectadas por eventos de este tipo.

Investiga las notificaciones de los sistemas de detección y monitorización

Los sistemas de detección y monitorización envían continuamente información sobre incidentes en las redes internas y externas.

Los sistemas modernos son completamente automáticos y son capaces de gestionar gran cantidad de información. Se hace imposible revisar todas las alertas pero, al menos, se debe asegurar que se investiga aquellas notificaciones que impliquen amenazas de mayor gravedad.

Comprende el impacto del incidente

Un alto nivel de madurez en la organización lleva a altos niveles de comprensión de los impactos que se prevén en los BCPs u otros documentos similares. Una buena cuantificación del impacto ayudará a priorizar actuaciones.

Se realizan análisis forenses

El análisis forense, nos permite saber que ha pasado o está pasando en nuestro sistema, detectando el punto de origen de la infección, quien lo ha realizado y que impacto atenido en el sistema.

Los incidentes se clasifican de acuerdo con los planes de respuesta

Los incidentes pueden suponer una pérdida de información, una interrupción de servicio, etc. En estos incidentes crear un marco de clasificación resulta útil para priorizar adecuadamente las actividades de respuesta a incidentes.

La clasificación también ayudará a derivar métricas significativas como tipo, gravedad, vector de ataque, impacto y causa raíz para futuras acciones de respuesta.

Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas o externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad)

El análisis de vulnerabilidad es el proceso mediante el cual se determina el nivel de exposición y predisposición a la pérdida de un elemento o grupos de elementos ante una amenaza específica. La finalidad es conocer qué vulnerabilidades existen en los sistemas de una compañía y de esa manera poder elaborar un plan de respuesta adecuado, desde fuentes internas o externas.

Mitigación

Los incidentes de seguridad, ¿quedan registrados y gestionados a nivel central?

Una vez que se ha comunicado el incidente de seguridad, el responsable de Seguridad deberá registrar formalmente dicho incidente, detallando toda la información básica del mismo: el tipo de incidente, descripción de este, fecha de la notificación, etc.

En el caso de que sea necesario, el responsable de Seguridad se coordinará con el responsable de Privacidad.

Junto al registro del incidente, se deberán registrar todas las actuaciones relacionadas con la gestión del incidente: las actuaciones de emergencia, las modificaciones del sistema derivadas del incidente; aquella evidencia que pueda, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos; etc.

Una de las soluciones más efectivas son las que permiten la gestión de la información sobre seguridad y gestión de eventos o SIEM (*Security Information and Event Management*) ya que proporciona una respuesta inmediata y eficiente ante los ataques que reciben las empresas contra sus sistemas informáticos.

Sin embargo, por sí solas no son suficientemente eficaces. Por eso, a su vez, se debe contar con ciertas bases sólidas para que la gestión de incidentes. P.e.: Nomenclatura de Activos, Inventario, Clasificación, *Ownership*, Relaciones/ Dependencias de los Sistemas, son elementos fundamentales y que impactan directamente en la adecuada gestión de incidentes.

Los incidentes son contenidos

A través de la contención se busca la detección del incidente con el fin de que no se propague y pueda generar daños de seguridad (p.e. ante un acceso no autorizado (incidente) como puede ser los sucesivos intentos fallidos de login, la respuesta (contención) podría consistir en bloquear

dicha cuenta; ante la infección de un virus (incidente), la respuesta (contención) podría ser la desconexión de la red del equipo afectado.

En cualquier caso, la empresa debe poseer una estrategia de contención previamente definida, para así poder tomar decisiones ágiles y acertadas.

Los incidentes son mitigados

Una vez que el incidente ha sido contenido se procederá a la erradicación de cualquier rastro dejado por el incidente como código malicioso.

En algunas ocasiones durante el proceso de se puede hacer necesario activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres), mencionados anteriormente, cuando el incidente en cuestión afecte gravemente a un determinado sistema.

El protocolo de gestión con aseguradora para responder al incidente incluyendo servicios o asesoramientos del asegurado (proveedor de seguridad de ciber de asegurado que conoce la red/equipos previamente).

Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados

La gestión de riesgos implica tomar decisiones. Y una de ellas es aceptar el riesgo. Aceptar riesgos no es malo, es sólo una decisión.

Cuando aceptamos un riesgo estamos diciendo que no actuamos preventivamente, es decir, que no vamos a hacer nada que pueda impedir que suceda. Sin embargo, sí que podremos actuar si ocurre.

Lo habitual es que, a pesar de no mitigarlo con controles, decidamos hacer un plan de contingencia, es decir, si el riesgo viene, desarrollamos una hoja de ruta que indique cuáles son las principales acciones que debemos tomar en esa situación.

Dado que la probabilidad y el impacto de un riesgo cambia a la misma velocidad que la del contexto de la organización, es aconsejable definir una periodicidad para revisar los riesgos aceptados.

Adicionalmente, todos los riesgos, aceptados o no, pero más aún si cabe si son aceptados, deben estar documentados. No sólo a nivel descriptivo, sino también en cuanto a la valoración y análisis que se ha hecho del mismo.

Mejoras

Los planes de respuesta incorporan las lecciones aprendidas

Por más que logremos contener el incidente a tiempo, si no logramos trabajar en las posibles causas que originaron el mismo, no estaremos haciendo las cosas bien.

El proceso de gestión de incidentes debe verse como una gran oportunidad de mejorar el gobierno de la seguridad de la información.

Las lecciones aprendidas sin el conocimiento adquirido en la gestión de incidentes y accidentes que permite determinar cómo se dio respuesta o cómo debería darse respuesta en el futuro con el fin de mejorar la gestión de estos.

Existen varios formatos para documentar lecciones aprendidas, dependiendo de los objetivos que se pretendan lograr, las audiencias a las que están dirigidos, el tiempo y los recursos disponibles.

Estos formatos pueden variar desde la mínima expresión escrita de una lección hasta informes completos de evaluaciones de impacto.

Estos aprendizajes deberán ser compartidos con la organización, empezando por los directamente involucrados y, a partir de ahí, con un lenguaje claro y resumido, al resto de la organización.

Se actualizan las estrategias de respuesta

Finalmente, mediante el análisis del incidente, es posible que haya que realizar un endurecimiento del sistema de seguridad que permita prevenir incidentes similares en el futuro.

Esto, en ocasiones, pasa por volver a visitar las estrategias de respuesta y ver si la organización decide aceptar los riesgos o mejorar sus capacidades internas tanto tecnológicas como de formación/capacitación del personal.

Fase 5 Recuperación

Esta fase tiene como objetivo devolver a la empresa a la situación previa al incidente, lo que podríamos denominar "volver a la normalidad". Hasta que se consiga esta situación, la empresa habrá estado funcionando de forma parcial y/o con ineficiencias, con el consiguiente impacto negativo en la cuenta de resultados y el posible daño a la imagen.

Como en general las pólizas ciber cuentan con una cobertura de pérdida de beneficios, los aseguradores tienen interés en que sus asegurados dispongan de planes que les permitan recuperar la normalidad en el menor tiempo posible, reduciendo el periodo y el coste de la pérdida de beneficios además del impacto del daño reputacional.

Disponer de estos planes no solo permite ahorrar tiempo, al tener definidos las tareas a realizar y las personas responsables de estas, sino que también mejorará la calidad de las decisiones tomadas o de los pasos ejecutados. Establecer la manera de actuar en situaciones de crisis, con una gran presión e incertidumbre, hace bastante probable que las decisiones tomadas sean mejorables. Este es objeto de estos planes: definir la manera más adecuada de actuar frente a una crisis, sin que se haya producido esta y disponiendo de tiempo para determinar la mejor manera de enfrentarse a ella. Por supuesto, si en un futuro se produce una crisis, las lecciones aprendidas deben ser una fuente para mejorar los planes definidos inicialmente.

Medidas

Planificación de la recuperación

Dispone de planes de continuidad de negocio

Un plan de continuidad de negocio (BCP) es un documento que define las reglas de primer nivel necesarias para reanudar las actividades empresariales ante un incidente disruptivo hasta conseguir recuperar la situación previa al incidente.

Disponer de estos planes, de los cuales ya hemos hablado en la fase anterior, reduce el tiempo para recuperar la normalidad y el impacto negativo que un incidente puede provocar en la imagen de la empresa.

Línea Roja Mercado Asegurador: Contar con un BCP adecuado es una de las nuevas líneas rojas que las aseguradoras están incluyendo en sus últimas directrices.

Dispone de planes de recuperación de sistemas

Los planes de recuperación formarán parte del plan de continuidad de negocio (aunque se pueden tener planes de recuperación sin que haya definido un plan de continuidad). Son planes en los que se detalla la forma de actuar ante situaciones específicas.

Dada la trascendencia de los sistemas de información en el contexto de un incidente cibernético, el fallo de los sistemas es una de las situaciones que se deben contemplar. En estos planes se detalla cómo recuperar los sistemas en distintos escenarios, uno de los cuales, en estos momentos, debe ser el de un ataque de ransomware.

Dispone de planes de gestión de crisis

Una crisis es un evento con alto grado de incertidumbre y múltiples consecuencias que impide que una organización logre sus objetivos, pudiendo poner en peligro su supervivencia. Hay que tener en cuenta que la gravedad

de una crisis depende tanto del evento que la origina como de la percepción del mundo exterior.

Un plan de gestión de crisis ayudará en la organización, dirección y comunicaciones durante la situación de crisis. Incluirá la estrategia, recursos y herramientas necesarias. La gestión de una crisis requiere una organización específica.

Durante la gestión de la crisis se determinará si es necesario activar los planes de continuidad de negocio.

Se exige a los proveedores críticos externos de IT que dispongan de planes de continuidad de negocio

Parte de las actividades críticas de una organización serán prestadas por proveedores externos. El efecto de disponer de planes internos para garantizar la continuidad de negocio queda limitado si un proveedor crítico sufre un incidente importante y este no dispone de planes para recuperar la actividad.

En consecuencia, los planes de continuidad que desarrollen las empresas deben complementarse con los que dispongan sus proveedores críticos para garantizar la recuperación tanto si el incidente se produce dentro de la organización como en alguno de sus proveedores críticos (esto no significa que los proveedores deban entregar sus planes de continuidad a sus clientes).

Los operadores de infraestructuras críticas de los sectores considerados estratégicos (transporte, telecomunicaciones, finanzas, energía, agua, sanidad…) deben cumplir con un reglamento que les obliga a disponer de planes de continuidad de negocio.

Se exige a los proveedores externos de IT algún tipo de indemnización

Si un proveedor es el causante del daño a una organización, esta debería poder reclamar al causante los daños y perjuicios que haya producido o permitir a la aseguradora repetir contra el causante.

La existencia en los contratos de cláusulas para fijar indemnizaciones o la inexistencia de cláusulas limitativas de responsabilidad reducirá en estos casos el coste del incidente.

CPDS

Dispone de Centros de Procesos de Datos (CPD) redundantes

La redundancia de medios es una herramienta habitual para gestionar incidentes. Disponer de centros de procesos de datos redundantes permitirá en relativamente poco tiempo, sino de forma inmediata, poder seguir dando servicio ante el fallo de uno de ellos.

Los centros redundantes se encuentran en ubicaciones diferentes y distantes en términos de riesgo

Un paso adicional para reducir el riesgo es que los centros se encuentren en ubicaciones diferentes y distantes. Esto reduce la probabilidad de que ambos puedan quedar inoperativos ante un incidente que afecten a un mismo lugar (atentado, incendio, inundación, terremoto, impacto de una aeronave, etc.).

Back ups

Los back ups se realizan de forma sistemática

La información de los sistemas es uno de los activos más importantes de una organización y como tal hay que protegerla. Una medida básica para proteger la pérdida de datos es realizar copias de seguridad (back up), siendo este un medio para recuperarse ante incidentes. Las copias deben realizarse de forma sistemática y con la suficiente frecuencia como para poder restablecer una situación próxima al momento en el que se produce el incidente.

La pérdida de información puede ser una de las situaciones más críticas a las que se enfrenten muchas empresas. Si se pierden máquinas, será posi-

ble sustituirlas con más o menos tiempo y más o menos dinero pero si se pierden completamente los datos, recuperarlos puede ser una cuestión que ni el tiempo o ni el dinero puedan resolver.

Redundancia de back ups offline / offsite

Un back up offlline es una copia de seguridad que se produce cuando las bases de datos están fuera de línea. Los servidores de respaldo de estos back ups se apagan hasta que se realizan nuevas copias o son necesarios para recuperar los datos.

Un back up offlsite es un back up que se realiza fuera de ubicación principal. Los datos se trasladan fuera bien de forma electrónica o a través de medios de almacenamiento extraíbles.

La redundancia de back ups reduce el riesgo de recuperación respecto a disponer de un solo back up. Además el offline reduce el riesgo de que los datos sean atacados y el offsite de que se vean comprometidos por daños en la ubicación principal.

Verificación de la continuidad de negocio

Prueba periódicamente los planes

Disponer de un documento que defina la operativa a seguir en caso de incidente, no garantiza que esta se cumpla cuando sea necesario activar los planes. También puede ocurrir que algo que bajo la teoría debería funcionar correctamente, no lo haga en la práctica. Y por último, la práctica facilitará la preparación para cuando surja la necesidad de activar los planes.

Revisa periódicamente los planes

Las empresas cambian y por tanto los planes también deben cambiar para adaptarse a esto. Confiar en que los planes nos permitirán gestionar una crisis y encontrarnos que, cuando esta se produce, están

obsoletos, no va a facilitar la gestión de la misma y añadirá tensión a la situación.

No basta con disponer de planes, es necesario revisarlos periódicamente para confirmar que siguen estando en vigor y proceder a actualizarlos en caso contrario. En los propios planes debe figurar quien es el responsable de su revisión y la periodicidad con la que es obligatoria hacerla.

Comunicación

Dispone de planes de comunicación para que las actividades de restauración se coordinen con partes internas y externas

La comunicación es un proceso fundamental durante la gestión de una crisis. Ya se ha indicado que una crisis requiere una organización específica, por lo que los canales de comunicación habituales puede que no sean de aplicación.

Tendremos necesidad de coordinar la actuación de forma ágil entre las distintas personas que toman las decisiones, los que intervienen en la solución del incidente, las posibles comunicaciones que haya hacer a efectos legales, el flujo de información para la toma de decisiones, etc.

Las personas implicadas en el asunto anterior pueden ser de dentro de la empresa, pero también pueden ser externas.

No hay que olvidar, dentro de la gestión, al Consejo de Administración.

Dada la importancia del flujo de información para la correcta resolución del incidente, es muy importante que se haya predefinido quienes son los distintos actores que deben intervenir y la coordinación entre estos, lo que se materializa en planes de comunicación específicos o en un apartado del plan de continuidad de negocio dedicado a este asunto.

Dispone de planes para gestionar la reparación de la reputación después de un incidente

La gravedad de una crisis depende también de la percepción del mundo exterior, por lo que es fundamental disponer de planes específicos, o un

apartado específico dentro de los planes de continuidad de negocio, que contemplen la reparación de la reputación.

Esta comienza con la manera en que se comunica el incidente, aunque no se disponga de toda la información necesaria. La gestión de la comunicación no debe limitarse a los clientes, o a la sociedad en general, sino también hay que hacer partícipes al personal y a los proveedores. Disponer de modelos de comunicación para cada parte puede ayudar a esta gestión.

Otros

Las plantas automatizadas pueden operarse manualmente

En el caso de plantas de producción, un fallo en los sistemas que las operan puede producir la paralización de estas hasta que se resuelva el incidente. Si estas pueden operarse manualmente, aunque se reduzca la productividad, se reduciría la pérdida de beneficios derivada del incidente cibernético.

Las plantas de producción son redundantes

Si los mismos productos se producen en plantas diferentes, la paralización de una de estas tendrá un impacto menor que si el producto de fábrica solo en un planta.

El stock es suficiente para mitigar la interrupción de negocios

Si la actividad realizada requiere productos físicos, disponer permanentemente de un nivel de stock mínimo que garantice la actividad durante un plazo suficiente (de acuerdo con el establecido en los planes de continuidad de negocio) reducirá la pérdida de beneficios originada por el incidente.

Mejoras

Los planes se mejoran con las lecciones aprendidas tras un incidente

Una vez superada la situación de crisis es recomendable hacer un análisis que nos permita conocer cómo se ha gestionado. Este análisis, que se debe plasmar en un documento, reportará los puntos fuertes y débiles de la empresa ante la crisis, dando lugar a unas lecciones aprendidas que deberán incorporarse a los distintos planes.

5. CONCLUSIONES

En un mercado asegurador cada vez más complejo y especializado, y en un ramo como el que nos ocupa, en el que la siniestralidad es elevada y la incertidumbre todavía muy alta, es muy importante realizar una apropiada gestión del riesgo. Las líneas anteriores pretenden guiar a aquellas personas no expertas en esta materia y enfocarlas hacia aquellos puntos en los que el mercado se centra a la hora de seleccionar a sus asegurados.

Hemos empezado mostrando cómo describir las características de la empresa y su entorno.

Tras ello hemos hablado de Identificación, y de lo importante que es establecer una cultura de ciberseguridad y desarrollar la percepción que tiene el conjunto de la organización del riesgo de seguridad cibernética. Este proceso que debe hacerse prestando especial atención a la descripción de los activos críticos y a la formación de los empleados en materia de prevención.

Hemos continuado nuestro análisis describiendo la Protección de nuestros sistemas. Este capítulo detalla la implementación de medidas para proteger los sistemas de la compañía e intentar evitar de la mejor forma posible que se produzca un incidente, lo que no siempre es posible por mucho esfuerzo que dediquemos en este punto. Actualmente, el sector asegurador pone el foco en esta sección, y será muy importante para poder conseguir una cobertura adecuada contar con MFA en todas las conexiones remotas, dedicar especial atención a la protección de las cuentas privilegiadas, segmentar las redes de la empresa y los sistemas por geografía y unidades de negocio, y mantener buenas políticas de gestión de copias de seguridad y parcheo de vulnerabilidades.

En la fase de Detección hemos definido las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad en una fase temprana del ataque, poniendo especial atención en los sistemas de monitorización de redes.

En el siguiente capítulo hemos hablado de Respuesta, tratando el desarrollo e implementación de actividades apropiadas para, una vez se ha detectado el incidente, tomar medidas de forma rápida y ordenada. En este caso debemos apuntar que un sistema de EDR es clave.

Finalmente, hemos detallado las medidas necesarias para una buena Recuperación. Esta fase se centra en devolver a la empresa a la situación previa al incidente lo antes posible, lo que no será posible sin un adecuado Plan de Continuidad de Negocio.

Tras la lectura de estas páginas esperamos haber aportado luz sobre lo que es una adecuada gestión de la ciberseguridad según la normativa NIST y sobre aquellas medidas a las cuales el mercado de seguros cibernéticos da mayor importancia.

Gracias a nuestros colaboradores

Platinum

COLINVEGAFLETES ABOGADOS
HERBERT SMITH FREEHILLS
MAPFRE
ventiv

Golden

grupo addvalora
AIG
Allianz
AON
AXA XL Insurance
Berkshire Hathaway Specialty Insurance
CHUBB
CLYDE&CO
DAC BEACHCROFT
GENERALI Global Corporate & Commercial
HDI
howden
Marsh
Munich RE
QBE
sedgwick
Swiss Re Corporate Solutions
wtw
ZURICH

Silver

FBAsociados
HASA
Liberty Specialty Markets
RSA
INTERNATIONAL SOS
HIGHDOME

El riesgo cibernético se sitúa entre los principales riesgos que preocupan a las empresas. Para poder hacerlo frente es imprescindible partir de la prevención, aunque esta no garantiza que no se esté expuesto e incluso pueda producirse un ciberataque, si no que, desde la prevención, la empresa conozca las medidas de detección, respuesta y recuperación para que el daño se contenga lo antes posible con el menor impacto.

La transferencia del riesgo a través de pólizas de seguro nos permitirá disponer de servicios que nos pueden ayudar a gestionar el siniestro además de reducir o cancelar el impacto económico de este. Pero esta transferencia no será posible si no disponemos de medidas adecuadas para prevenir y responder ante incidentes tecnológicos.

Para ello, se ha elaborado esta guía, cuyo objetivo principal es trasladar fundamentalmente al colectivo de gerentes de riesgos y/o seguros, pero también a todo el personal no técnico implicado en estos riesgos, qué medidas de diversa índole son recomendables para gestionar la prevención de los incidentes cibernéticos.