COVER grup

CORREDURIA DE SEGUROS

PROTOCOLO CIBERSEGURIDAD

🛡️ Protocolo de Actuación ante un ataque informático

INTRODUCCIÓN Y OBJETIVO

Este protocolo tiene como finalidad establecer unas pautas para la correduría ante un Ciber incidente que pueda comprometer los datos personales, operaciones o la continuidad del negocio.
Las diferentes acciones de respuesta se verán condicionadas por el tipo de incidente.

ROLS Y RESPONSABILIDADES

Antes de cualquier incidente, hay que tener en cuenta los roles mínimos de respuesta establecidos por la correduría

- Responsable del incidente: Meri Gutiérrez
- Responsable técnico o proveedor informático: TIC BCN
- Asesor RGPD o DPD: Isabel Martos (J2M Consultores)
- Responsable de comunicación: Dani Bonamusa
- Responsable de contacto con la póliza de Ciberriesgos: Meri Gutiérrez

1️⃣ FASE DE PREVENCIÓN

Objetivo: Reducir el riesgo a partir de un ataque informático.

Acciones recomendadas:

- Formación continua básica a todos los empleados sobre ciberseguridad.
- Simulaciones periódicas de phishing a los empleados.
- Uso de contraseñas robustas y cambio periódico.
- Uso de antivirus actualizado en todos los dispositivos.
- Actualizar regularmente las aplicaciones y sistema operativo.
- Activación de doble autenticación a los servicios en línea que lo permitan (MFA), en especial al ERP y correo electrónico.
- Revisión periódica de los permisos de los usuarios, eliminar accesos de personas que ja no trabajan en la Correduria y aplicar el principio del mínimo privilegio a los sistemas críticos como el correo, ERP, webs aseguradoras y herramientas bancarias.
- Revisión periódica de los sistemas con el proveedor informático.
- En el correo electrónico se recomienda la activación del MFA, revisar reglas de reenvío automático, bloquear accesos sospechosos y limitar el uso de buzones compartidos sin control.
- Formación a los empleados para que verifiquen cambios de cuenta bancaria, solicitudes urgentes o instrucciones recibidas por canales no habituales.
- Establecer copias de seguridad propias, en especial de la información de valor almacenada localmente y mantenerla de forma desconectada de la red.
- Contratación de una póliza de ciber riesgo con asistencia especializada y revisarla periódicamente.
- Inventariar los activos digitales y los datos sensibles.
- Disponer de la lista de contactos de emergencia actualizada.

2️⃣ FASE DE DETECCIÓN, DETERMINACIÓN DEL ALCANCE Y PRIMERAS ACCIONES

Objetivo: Identificar si se ha producido un ataque, alcance y tomas las primeras acciones.
Síntomas habituales de un incidente (entre otros)**:**

- Ordenador lento o bloqueado.
- Mensajes extraños, ventanas emergentes y/o pop ups inesperados y/o sospechosos
- Programas o aplicaciones que se ejecutan solos o con comportamientos extraños.
- Correos enviados que no se han escrito.
- Acceso denegado a sistemas habituales y/o cambios no autorizados en contraseñas o permisos.
- Ficheros encriptados, modificados o con nombres extraños.
- Redireccionamientos desconocidos al navegar.
- Comunicación del incidente por parte del proveedores o clientes.

Acciones inmediatas:

- **Mantener la calma y actuar con método.**
- Comunicar al responsable de gestionar la incidencia y al portavoz para gestionar la comunicación.
- Identificar el incidente y evaluar el alcance de este (ERP, correo, dispositivos locales,…)
- **Desconectar el dispositivo de la red (Wifi o cable)**, para evitar el riesgo de propagación.
- Guardar para un posterior registro: correos sospechosos, capturas de pantalla, mensajes de error, nombres e ficheros infectados, direcciones IP o dominios sospechosos, tomando fotografías si es necesario.
- **Valorar si apagar o no el dispositivo.**
  La decisión dependerá de:
  - El tipo de dispositivo (ordenador, servidor, móvil, etc.).
  - Si contine información almacenada localmente.
  - El tipo de incidente (ransomware, acceso no autorizado, malware, etc.).
  - Si se dispone de soporte técnico especializado para analizar el sistema en caliente.

  No apagar el dispositivo si:
  - Se quiere preservar evidencias digitales para un análisis forense (logs, procesos activos, conexiones,…)
  - Se dispone de soporte técnico o herramientas para analizar el sistema en funcionamiento (live response).
  - La actividad maliciosa observada no está eliminando, ni encriptando, ni filtrando/enviando datos de forma activa.

Apagar el dispositivo si:

- Se detecta un proceso malicioso activo que esta eliminando, encriptando o filtrando/enviando datos.
- No se dispone de soporte técnico inmediato y se quieren evitar más daños.

- **Bloquear al usuario o cambiar la contraseña inmediatamente,** desde un dispositivo limpio, **si se detecta acceso no autorizado al correo, bancos, webs aseguradoras, redes sociales o ERP.**
- Cuando haya sospecha de una cuenta comprometida, además de cambiar la contraseña desde un dispositivo limpio, hay que cerrar las sesiones activas, revocar los accesos o tokens si el sistema lo permite, revisar las reglas de correo, reenvíos, dispositivos vinculados y recuperaciones de contraseña, y comprobar si se han creado usuarios o permisos no autorizados.
- Comunicar el incidente a empleados, para su información y que extremen las precauciones.
- Contactar con el **servicio de asistencia de la póliza de ciber riesgo,** en caso de tenerla disponible.
- Consultar a Incibe o Agencia de Ciberseguridad de Catalunya en caso de que sea necesario.
- Consultar con el **asesor RGPD** para valorar el impacto legal y las obligaciones de notificación, en cas de tener el servicio contratado.

3 FASE DE CONTENCIÓN

Objetivo: Evitar que el ataque se esparza.
Acciones:

- Desconectar otros dispositivos sospechosos.
- Bloquear el acceso a cuentas comprometidas
- Desconectar servidores locales (si hay): Apagar servidores físicos y aislarlos de la red hasta que se pueda analizar el incidente.
- Desactivar sincronizaciones con la nuve: Servicios como OneDrive, Sharepoint,..., pausar la sincronización para evitar que ficheros infectados se propaguen.
- Desactivar los accesos remotos: Herramientas como TeamViewer, AnyDesk o accesos a RDP, desactivarlos temporalmente para evitar intrusiones externas.

4 FASE DE COMUNICACIÓN

Objetivo: Informar a las partes implicades.
Internamente:

- Asegurarse que todo el personal interno dispone de la información.

Externamente (según con las indicaciones del asesor RGPD)**:**

- Autoridades (como AEPD si hay datos personales afectados, en que el plazo es de 72 horas desde conocimiento del incidente).
- Clientes (si hay afectación de datos de alto riesgo): no hay un plazo fijado, pero debe realizarse sin dilación indebida.
- Proveedores tecnológicos.

Las comunicaciones externas deben ser claras, prudentes y coordinadas. Antes de informar a clientes o proveedores, hay que validar el mensaje del asesor de RGPD, el responsable del incidente y póliza de Ciberriesgos. La comunicación tiene que explicar que ha pasado, que datos o servicios han podido estar afectador, que medidas se han tomado y que canal de contacto se habilita.

5️⃣ FASE DE RECUPERACIÓN

Objetivo: Volver a la normalidad con seguridad.
Hay que revisar si la Correduria puede seguir operando durante la incidencia: accesos alternativos a correo, teléfonos de contacto, canales con compañías, acceso a ERP, gestiones urgentes.
Acciones:

- Restaurar las copias de seguridad.
- Validar la integridad del sistema.
- Revisar sistemas con el proveedor informático.
- Documentar el incidente y las acciones realizada.
- Monitorizar posibles nuevos intentos de ataque.
- Comunicar el post incidente a clientes, proveedores, autoridades, … a los que se haya notificado previamente.

6️⃣ FASE DE PREVENCIÓN FUTURA

Objetivo: Reducir el riesgo de futuros ataques.
Después de cerrar un incidente, hay que hacer una revisión de las decisiones tomadas y aprendidas con el proveedor informático, el asesor de RGPD en caso de que sea necesario y todas las personas implicas. Esta revisión tiene que generar un plan de acción con medidas concretas, responsable y plazos de: mejora técnica, formacion adicional, cambios de permisos, revisión de copias, actualización de protocolo y pruebas periódicas.

Acciones:

- Analizar el origen del incidente y adoptar las medidas adicionales razonables.
- Revisar, y adaptar si hace falta, el protocolo de actuación.
- Revisar, y ampliar si hace falta la póliza de ciber riesgo.

Lista de contactos de emergencia

- **Asistencia de la póliza de Ciber Riesgo:**
  Compañía: Stoïk
  Número de póliza: ESAXTMST250312227577
  Tel: +34 911 67 63 42 (disponible 24h – 365 días)

- **Servicio de asesoría sobre RGPD:**
  Empresa: J2M Consultores Informáticos, Sl
  Pers. Contacto: Isabel Martos
  Tel: 651 18 32 06
  Email: imartos@j2mconsultores.com

- **Servicio Informático:**
  Empresa: TICBCN CONSULTORS SL
  Pers. contacto: Pere Torres
  Email: pere@ticbcn.com
  Tel: 695 553 110 / 93 741 22 82

- **ERP: MPM Software**
  Help Desk**:** Telf : 938 053 929

- **Incibe** (Instituto Nacional de Ciberseguridad):
  Web: https://www.incibe.es/
  Tel: 017 y 900 116 117
  WA: 900 116 117

- **Agencia de Ciber seguridad de Catalunya:**
  Web: https://ciberseguretat.gencat.cat/ca/inici
  Tel: 900 112 444
  Email: cert@ciberseguretat.cat

☑ Check-list rápida – Fase 1

🔍 FASE 1 – Prevención

✓	Acción
☐	MFA activado en los servicios críticos: correo electrónico, ERP, banca y portales de aseguradoras.
☐	Copias de seguridad verificadas con pruebas de restauración documentada.
☐	Contactos de emergencia actualizados: proveedor informático, Ciberriesgos, RGPD y organismos de soporte.
☐	Permisos de usuarios revisados y accesos de antiguos trabajadores eliminados.
☐	Póliza de Ciberriesgos revisada y canales de asistencia identificados.
☐	Simulaciones de phishing y formación periódica planificadas.

☑ Check-list rápida – Fases 2 a 4:

"Mantener la calma y actuar con método."

🔍 FASE 2 – Detección y primeras acciones

✓	Acción
☐	**Informar al responsable de gestionar la incidencia.**
☐	**Identificar síntomas** (ordenador lento, ficheros encriptados, mensajes extraños, etc.)
☐	Identificar el incidente y evaluar el alcance.
☐	**Desconectar el dispositivo de la red (Wifi o cable)**
☐	Hacer capturas de pantalla o fotos de los mensajes o errores
☐	**Valorar si hace falta apagar el dispositivo**
☐	**Bloquear cuentas o cambiar contraseñas** desde un dispositivo seguro. Si hace falta cerrar sesiones activas, revocar accesos o tokens, revisar reglas de correo, reenvíos, dispositivos vinculados y de recuperación de contraseña, comprobar si se han creado usuarios o permisos no autorizados.
☐	**Informar internamente a todo el personal**
☐	**Contactar con el servicio de asistencia de la póliza de ciber riesgo**
☐	Contactar con INCIBE o Agencia de Ciber seguridad, si hace falta
☐	Consultar con el asesor de RGPD para valorar notificación a AEPD o afectados

🛑 FASE 3 – Contención

✓	Acción
☐	Desconectar otros dispositivos sospechosos
☐	Bloquear el acceso a cuentas comprometidas
☐	Apagar o aislar servidores locales (si hay)
☐	Pausar sincronizaciones con la nube (OneDrive, SharePoint, Dropbox…)
☐	Desactivar accesos remotos (TeamViewer, AnyDesk, RDP…)

FASE 4 – Comunicación

✓	Acción
☐	Informar a todo el personal interno
☐	Notificar a AEPD si hay datos personales afectados (dentro de las 72 h)
☐	Informar a los afectados si hay alto riesgo para sus datos (sin dilación indebida)
☐	Informar proveedores tecnológicos implicados

Check-list rápida – Fases 5 y 6

FASES 5 y 6 – Recuperación y prevención futura

✓	**Acción**
☐	Restaurar las copias de seguridad, validando previamente que no estan comprometidas.
☐	Comprobar la integridad de los sistemas restaurados.
☐	Reactivar accesos de forma gradual y controlada.
☐	Monitorizar posibles recurrencias y/o nuevos intentos de ataque.
☐	Documentar el incidente y acciones tomadas.
☐	Comunicar el cierre del incidente si previamente se ha informado a clientes, proveedores o autorizades.
☐	Documentar lecciones aprendidas y definir un plan de acción de mejoras con responsables y plazos.

🛡️ Prevención y gestión incidentes póliza ciber Stoïk

1. Prevención a través de Stoik Protect

Se puede acceder a la plataforma de prevención Stoïk Protect (https://www.stoik.io) durante todo el periodo de seguro. Dispone de las siguientes herramientas de prevención:

- **Escaneo externo:**
  Cada semana se realiza automáticamente una auditoría de la superficie externa del sistema informático.
- **Análisis interno:**
  Análisis de las configuraciones de los entornos Cloud Azure y AWS y del Active Directory.
- **Simulación de phishing :**
  Falsos correos electrónicos de phishing para formar a sus equipos en la detección de mensajes fraudulentos.
- **Módulos de formación:**
  Tutoriales sencillos y prácticos para formar a sus equipos en buenas prácticas cibernéticas.

2. Gestión de Incidentes

Se debe notificar el descubrimiento lo antes posible.

Tras la **notificación** de un **incidente cibernético potencial**, o de un **incidente cibernético real**, Soïk designará a un **gestor de crisis** en las dos horas siguientes a la notificación. Esta persona se encargará de coordinar la intervención de los siguientes **consultores especializados**:

- Un **experto informático**, cuya función, en caso necesario, es:
  - Identificar, analizar, contener y poner fin al incidente cibernético
  - Determinar en qué medida el incidente cibernético ha comprometido o causado la pérdida, destrucción o deterioro de sus datos o sistema informático.

- Un **asesor jurídico** encargado, en su caso, de:
  - Asesorar sobre la obligación de notificación y tramitación ante la autoridad administrativa; 4 Condiciones Generales
  - Asesorar sobre las obligaciones de notificación a las personas afectadas
  - Redactar el texto de la notificación a las personas afectadas o a la autoridad administrativa cuando dichas notificaciones sean necesarias.

- Un **asesor de comunicación** de crisis cuya función, en caso necesario, consistirá en elaborar y poner en marcha una campaña de relaciones públicas destinada a evitar o limitar los daños a su reputación como consecuencia del incidente cibernético, y en su caso, hacer recomendaciones concretas para reestablecer su reputación.