CHRISTIAN **DUMONT**

Préface de **Dominique Moisand**

ITIL

pour un service informatique optimal

ISBN : 2-212-11734-5

EYROLLES

Chapitre 6

La gestion des incidents

Quelles que soient la qualité du système d'information mis en place dans l'entreprise ou les compétences des techniciens qui l'exploitent, des incidents se produiront. Ces incidents ont toujours un effet important sur la confiance que les utilisateurs accordent à l'équipe qui gère ce système d'information. La manière de gérer ces « crises » et la rapidité de leur résolution est un révélateur de la maturité de l'équipe informatique. C'est pourquoi l'implantation du processus de gestion des incidents, véritable fer de lance du centre de services, est particulièrement importante.

Vue d'ensemble

Selon ITIL, un incident peut être défini comme tout événement ne faisant pas partie du fonctionnement normal d'un service (ou d'un équipement) et qui cause ou peut causer une interruption du service ou une altération de sa qualité.

En conséquence, le but principal de la gestion des incidents est de rétablir le fonctionnement normal du service aussi vite que possible et d'en minimiser l'impact pour l'entreprise, tout en assurant le meilleur niveau de disponibilité et de service possible, tel qu'il est défini dans le contrat de service (SLA).

Il s'agit donc de traiter les conséquences et non les causes…

Pourquoi une gestion des incidents ?

Dans un système de support non géré, la fréquence des interruptions est un facteur particulièrement déstabilisant pour les membres de l'équipe technique, ce qui entraîne une baisse d'efficacité. Cette conséquence est aussi largement constatée chez les utilisateurs qui, lorsqu'ils ne trouvent

pas de techniciens pour les aider, ont recours à leurs collègues et les interrompent régulièrement avec les mêmes effets sur la productivité.

De plus, si personne ne gère les incidents, personne n'est en mesure de mettre en place un système d'escalade afin d'éviter qu'un incident mineur au départ ne devienne plus critique et affecte la qualité de service.

Lorsque la solution à un incident est connue d'un technicien, si un autre membre de l'équipe est sollicité pour le résoudre, il est possible qu'il lui soit nécessaire de reprendre tout le processus de recherche avant d'arriver à la résolution au lieu de profiter de l'expérience de son collègue.

Tous ces éléments permettent de conclure que la gestion des incidents au sens ITIL a plusieurs avantages. En évitant la dispersion des techniciens sans contrôle et en leur évitant de gérer les utilisateurs en frontal, ce processus permet d'optimiser l'utilisation des ressources matérielles et humaines impliquées dans le processus de support. Cela permet également de garantir qu'un suivi efficace des incidents est réalisé, et qu'un historique des incidents et de leurs solutions permet de capitaliser et de partager l'expérience des différents techniciens. Enfin, la mise en place d'une gestion formelle des incidents permet de développer et d'appliquer une approche systématique du traitement des incidents, et d'éviter la perte d'incidents...

Comme exemples d'incident, on peut signaler la panne de matériel, l'indisponibilité d'une application, un ralentissement du réseau, ou un manque d'espace disque. Mais tous ces incidents renvoient à des dysfonctionnements ou des non-respects du niveau de service négocié avec l'utilisateur.

Dans la pratique, on considère également que toutes les demandes concernant la mise en place d'un nouveau service, d'une application, d'un matériel ou même les demandes concernant l'évolution de ce service, ainsi que toutes les demandes d'assistance simple, de formation ou autres, sont en fait des incidents et doivent être traités comme tel.

Concepts

La plupart des membres de l'équipe informatique participent à la prise en charge des incidents ou au contrôle des étapes de leur résolution. Mais dans les faits, c'est bien le centre de services qui assume la responsabilité de tous les incidents.

Comme signalé plus haut, le but de la gestion des incidents est de rendre disponible le service le plus rapidement possible. Ainsi, lorsque l'incident est déclaré au centre de services, l'équipe en charge de la résolution doit identifier si possible les causes de l'incident en faisant usage de la base de connaissances afin de trouver une solution.

Si l'incident ne peut être résolu rapidement par l'utilisation d'une solution définitive ou par un moyen de contournement, l'incident doit être transféré au niveau de support supérieur.

Une fois l'incident résolu et après restauration du service dans les termes du niveau de service négocié avec les utilisateurs (SLA), l'incident est considéré comme terminé, et son statut est donc mis à jour dans la base (CMDB).

Le statut d'un incident indique sa position dans le flux des traitements. Cette indication est communiquée à toutes les personnes concernées par cet incident. Aussi, est-il indispensable que chacun utilise le même vocabulaire avec des termes comme « nouveau, planifié, assigné, résolu ou fermé » et comprenne l'implication de la situation d'un incident en fonction de son statut.

Lors de la gestion de l'incident, il est important que le dossier de l'incident soit conservé afin que n'importe quel membre de l'équipe de service puisse fournir à un client un compte rendu à jour avec les détails des actions et de leurs résultats, du temps passé, des éventuelles procédures d'escalades, etc.

Lors de l'audit d'un incident, et surtout dans le cas d'une rupture du SLA, il est indispensable de pouvoir auditer les événements qui se sont produits sur la base du support. Afin de réaliser cet audit dans les meilleures conditions, plusieurs informations doivent être consignées dans la fiche de l'incident. Il est indispensable de pouvoir identifier les éventuelles modifications apportées à cette fiche lors des différentes interventions des techniciens. En particulier, on s'attend à trouver le nom de la personne ainsi que la date et l'heure de la modification. Mais on souhaite également savoir ce que la personne a modifié, le temps qu'elle y a consacré et la raison de cette modification.

Les différents niveaux d'escalade

Le premier niveau de résolution des incidents est le centre de services. Si celui-ci ne parvient pas à résoudre rapidement un incident, une procédure d'escalade est engagée. Cette procédure correspond au transfert de l'incident à un niveau de support supérieur (second, troisième niveau, etc.) composé de spécialistes qui disposent de plus de compétences et de temps pour trouver une solution au dysfonctionnement.

Ce type d'escalade « fonctionnelle » permet de disposer de plus de ressource dans la résolution de l'incident. Mais il existe également une escalade « hiérarchique » qui est activée lorsqu'une décision doit être prise concernant la résolution d'un incident, et en particulier lorsqu'il est nécessaire de faire intervenir une ressource externe.

Établissement des priorités

La gestion d'incident demande la mise en place d'un système d'ordonnancement basé sur un critère de priorité. Celui-ci est calculé en fonction de deux éléments qui sont l'urgence et l'impact.

L'urgence est une évaluation de la criticité de l'incident par rapport à l'activité de l'utilisateur et reflète la rapidité nécessaire à la résolution d'un incident.

L'impact concerne davantage le volume et l'ampleur de l'incident sur l'entreprise. On le mesure en général en exprimant le nombre d'utilisateurs ou le nombre de systèmes touchés par un dysfonctionnement. L'utilisation de la base CMDB permet de calculer plus efficacement l'impact d'un incident sur le système d'information, puisqu'elle recense le nombre d'utilisateurs d'une application, d'un matériel ou d'un service.

Lorsqu'un incident présente un impact majeur pour un grand nombre d'utilisateurs, on considère qu'il s'agit d'un incident majeur. Dans ce cas, une réunion spéciale est mise en place par l'équipe de la gestion des incidents avec la participation de toutes les personnes, en interne et en particulier des autres processus comme la gestion des problèmes ou provenant des fournisseurs extérieurs, susceptibles d'aider à rétablir la situation.

Périmètre

Le centre de services a le rôle central dans le processus de gestion des incidents.

Son rôle va de la détection et l'enregistrement des incidents à la surveillance de leur évolution. Le centre a également la responsabilité du classement de tous les incidents et distribue les tâches aux différents techniciens. Les membres du centre de services peuvent parfois s'occuper également du support initial de premier niveau, en s'appuyant sur la base de connaissances et les solutions identifiées (CMDB).

Pour les problèmes non résolus, les techniciens ont alors la mission de réaliser la recherche et le diagnostic de l'incident en vue de lancer la résolution de celui-ci et la reprise du service.

Après clôture de l'incident, le centre de services doit s'assurer de la mise à jour de la base de données CMDB et doit prévenir l'utilisateur du résultat des actions menées par les techniciens.

Terminologie

Très souvent, la cause d'un incident est apparente et peut être traitée immédiatement (exemple : plus de papier dans l'imprimante), mais il arrive parfois que cette cause ne soit pas identifiable simplement. Dans ce cas, une solution de contournement peut être proposée à l'utilisateur

(exemple : relancer l'ordinateur en cas d'erreur). Celle-ci permet de rendre le service disponible, mais ne résout pas le problème qui a de grandes chances de se représenter.

On définit alors le vocabulaire suivant :

Un *problème* est la cause inconnue d'un ou plusieurs incidents.

Une *erreur connue* est un problème dont les symptômes sont identifiés mais pour lequel aucune solution définitive ne s'applique, autre qu'une solution palliative permettant de rendre le service de nouveau disponible, ou lorsqu'une solution définitive est identifiée mais que la mise en place de la demande de changement n'est pas encore réalisée.

Une *demande de changement* ou RfC (*Request for Change*), correspond à la demande de mise en place de la solution à un problème sur un composant ou un service du système d'information. Celle-ci est examinée par le processus de gestion du changement avant mise en œuvre.

Figure 6-1 : Relation entre les incidents, les problèmes et les erreurs connues

Comme l'illustre la figure 6-1, Si aucune solution immédiate n'est possible, la gestion des incidents fait appel à la gestion des problèmes. Cette action qu'il ne faut pas confondre avec le système de l'*escalade* décrit plus avant, permet de modifier le flux du traitement de la défaillance en l'identification du problème, la recherche d'une solution palliative qui transforme le problème en erreur connue, puis la mise en place d'une demande de changement. Une fois la demande de changement appliquée sur le système d'information, la solution doit être enregistrée dans la base de connaissances (CMDB) et l'incident peut être corrigé définitivement.

Lorsqu'un nouvel incident est signalé, il doit être comparé aux incidents, problèmes et erreurs connues répertoriés dans la base. Les solutions de contournement disponibles sont appliquées afin d'apporter la résolution la plus rapide de l'incident.

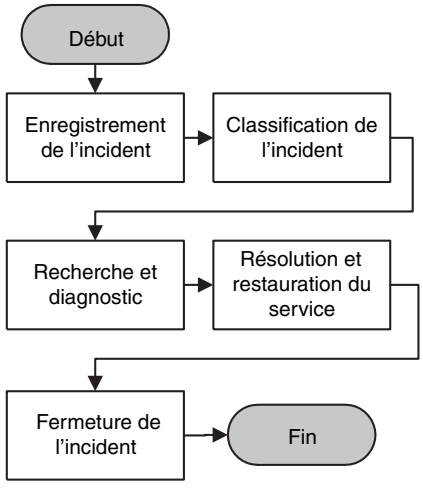
Cette base de connaissances doit être maintenue à jour régulièrement afin de ne conserver que les enregistrements qui apportent une valeur ajoutée au centre de services.

Description du processus

Flux du processus

Comme l'illustrent les figures 6-2 et 6-3, après détection ou déclaration de l'incident, le centre de services débute son action par l'enregistrement du contexte de l'événement (symptômes, premier diagnostic, information sur l'utilisateur et la configuration). Ces premiers éléments permettent entre autres de déterminer si cet incident s'est déjà produit et s'il s'agit d'une erreur connue avec une solution palliative, ou éventuellement une solution au sein de la CMDB. Dans ce cas, l'utilisation de cette solution permet de gagner un temps considérable.

Figure 6-2 : Flux simplifié du processus de gestion des incidents



L'étape suivante consiste à évaluer la priorité qui va être associée à l'incident en fonction de l'urgence de la situation et de l'impact sur le système d'information. Celle-ci va déterminer les ressources qui seront attribuées à la résolution.

La résolution de l'incident peut très bien se faire dès les premiers instants par le premier niveau en utilisant la base de connaissances et de configuration (CMDB) dans laquelle se trouvent des informations sur les incidents du même type, les erreurs connues et leurs solutions palliatives ou encore des solutions définitives. En l'absence de solution, une priorité de traitement est déterminée et on détermine les compétences nécessaires pour résoudre le dysfonctionnement. Ensuite, si nécessaire, un technicien se voit attribuer le traitement de l'incident sur le site incriminé.

Lorsqu'un problème sans solution est identifié par le technicien, le centre de services communique l'information à l'équipe de gestion des problèmes.

Même si la responsabilité de la résolution à été transférée à un autre groupe de spécialistes, le centre de services garde la responsabilité de l'incident et doit le gérer jusqu'à sa clôture et la satisfaction du client.

Après avoir identifié une solution à l'incident, celle-ci est appliquée en vue de résoudre le dysfonctionnement, puis une éventuelle restauration des données est démarrée afin de rendre le service de nouveau disponible.

Lorsque l'incident est résolu, avec l'accord de l'utilisateur, le centre de services doit clôturer l'intervention et s'assurer que le rapport d'incident est correctement rempli avec le détail des actions et de la solution mise en œuvre, le temps passé et les coûts associés.

Cet événement est sensible puisqu'il détermine l'instant où l'utilisateur est censé être satisfait. Dans les faits, il arrive que celui-ci ne perçoive pas la situation de la même façon. S'ensuit alors une négociation entre l'utilisateur et le centre de services avec une éventuelle réouverture de l'incident.

Le centre de services assume la responsabilité de la gestion des incidents et doit en conséquence contrôler le déroulement de leurs résolutions tout en informant l'utilisateur. Ce contrôle doit s'effectuer en surveillant le statut et la progression de chaque incident ouvert, et en particulier ceux qui transitent entre plusieurs groupes de spécialistes afin d'éviter l'effet « ping-pong ».

Comme on a pu le voir précédemment, deux modes de gestion peuvent coexister dans le traitement des incidents. Le premier correspond aux principe d'escalade. Si un incident ne parvient pas à être réglé rapidement, et lorsque l'on craint de dépasser le délai négocié du SLA, il est indispensable de changer le statut de cet incident afin de lancer la procédure d'escalade (fonctionnelle ou hiérarchique). Ce type de traitement ne doit pas être confondu avec la gestion des problèmes qui prend en compte le coté récurrent d'un incident. Dans ce cas, lorsque la résolution d'un dysfonctionnement impose un changement dans la configuration, il peut être nécessaire d'imaginer une solution de contournement. Cette solution de contournement doit alors être examinée par le processus de gestion des problèmes, puis approuvée avant sa mise en œuvre, sans oublier de mettre à jour la base CMDB afin que tous les techniciens aient connaissance de cette nouvelle solution, même s'il ne s'agit que d'un palliatif.

Si aucune solution n'est trouvée pour un incident, il se peut qu'il soit nécessaire de rencontrer plusieurs fois ce dysfonctionnement avant d'identifier un problème.

La classification est certainement la phase la plus importante de la gestion des incidents. Elle permet de déterminer quel est le service, l'application ou le matériel impliqué, les personnes touchées et ainsi d'appréhender l'ampleur, donc l'impact de l'incident. En disposant des informations du contrat de service, la classification permet de préciser les délais de restitution garantis et les fonctions prioritaires. La classification permet également de préciser les ressources nécessaires lors de l'investigation en vue de résoudre cet incident, et en particulier les spécialistes qu'il convient de mobiliser.

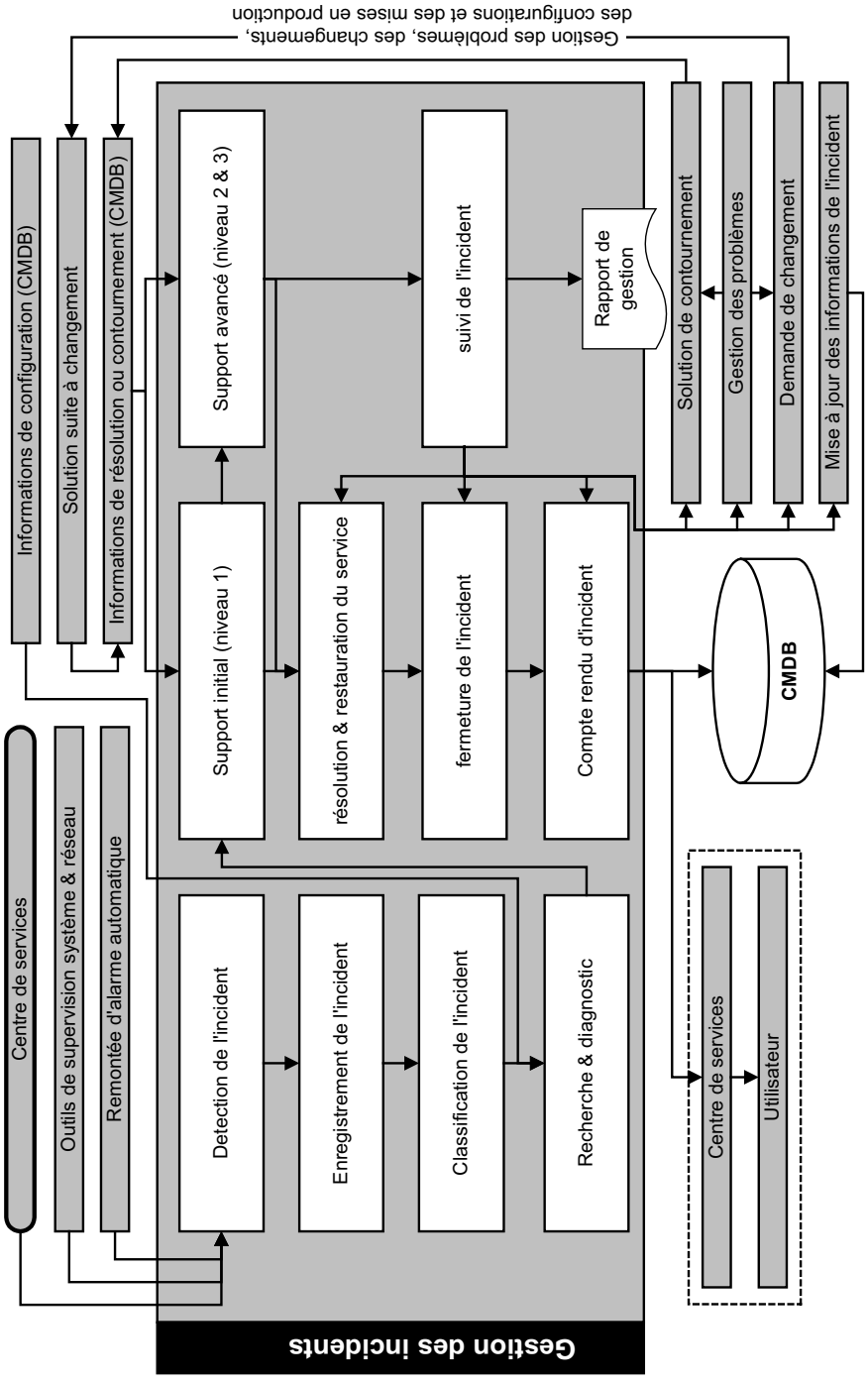


Figure 6-3 : Activités de la gestion des incidents

Planification et mise en œuvre

La mise en place d'un processus de gestion des incidents ne peut se faire sans la présence d'un centre de services. Mais au-delà de ce centre, la mise en place des autres processus de support, comme la gestion des problèmes, la gestion du changement et la gestion des configurations, est indispensable. Cependant, la gestion des incidents est le processus qui offre le meilleur retour sur investissement, ce qui est loin d'être négligeable lorsque son implantation donne lieu à quelques grincements de dents. La mise en place d'un centre de services et de la gestion des incidents peut prendre plusieurs mois. Aussi on aura tout intérêt à prévoir la création de ce centre dès le début d'un gros projet informatique, afin que l'importance du centre croisse avec celle du projet, avant de revenir à un équilibre raisonnable.

Améliorations

Des améliorations peuvent être obtenues par la formation des techniciens « classiques » dans le but de leur faire prendre conscience de leur rôle auprès des utilisateurs.

Des améliorations peuvent également provenir de la mise à jour régulière de la base de gestion des configurations (CMDB), et de la base de données des connaissances, permettant de recouper les informations concernant les erreurs connues, leurs résolutions et les solutions de contournement.

Une application informatique de gestion des incidents est indispensable. Il existe désormais des outils de support automatiques et efficaces disposant de systèmes experts pour la classification des incidents, mais également de procédure d'escalade automatique, de base de connaissances sur les incidents et leurs solutions.

Mesures et contrôles

Les métriques que l'on peut mettre en place pour valider l'efficacité du processus proviennent essentiellement du centre de services et concernent le nombre et la durée des incidents, leurs impacts sur le système d'information, et le ratio entre incidents résolus au premier niveau et ceux qui ont été transférés vers les supports de niveaux 2 et 3.

Documents et rapports de gestion

À l'instar des rapports du centre de services dont ils proviennent, les rapports de gestion doivent s'adresser à plusieurs publics tels que les responsables des directions fonctionnelles, les membres de la direction générale, les responsables de l'informatique, mais également les représentants des utilisateurs eux-mêmes.

Conséquences

Les conséquences générées par la gestion des incidents sont multiples et agissent sur plusieurs niveaux de l'entreprise. D'un point de vue général, on constate une réduction de l'impact des incidents par la rapidité de la résolution, ainsi que par la détection proactive de ces incidents, ou par les améliorations qui devraient être appliquées afin de les éviter. De plus, on dispose à présent d'informations plus orientées gestion et portant sur les niveaux de SLA qui vont permettre par la suite de valider l'efficacité du processus et son adéquation avec le métier de l'entreprise. Au niveau de l'organisation de support, les avantages sont plus liés aux gains en efficacité de l'équipe technique du fait de l'utilisation plus rationnelle des ressources, de la capitalisation de l'expérience de chacun, mais également par la réduction des interruptions individuelles des techniciens sollicités en direct dans les couloirs. On constate également une nette diminution puis l'élimination totale des pertes de demandes des utilisateurs, ce qui se produisait inévitablement lors de la génération Post-it !

Mais ces avantages sont également liés à la qualité des informations qui composent désormais la base de connaissances du service (CMDB), ce qui permet sans nul doute de valider plus efficacement les éléments communiqués par l'utilisateur lors de la déclaration de l'incident, puis d'accélérer la recherche d'information sur la configuration incriminée. Cette base de connaissances procure ensuite une documentation indispensable à la capitalisation de l'expérience des techniciens.

Enfin, et c'est certainement le plus important, de tout ceci découle une plus grande satisfaction des utilisateurs.

Malheureusement, avant d'arriver à cette situation idyllique, plusieurs écueils sont fréquemment rencontrés. Le plus classique d'entre eux est sans nul doute la résistance au changement qui montre systématiquement son visage dès l'installation d'un nouveau processus. Dans le cas de la gestion des incidents, cette résistance au changement est fortement liée à l'implantation du centre de services. La conséquence immédiate peut s'exprimer par une désaffection des utilisateurs qui refusent d'utiliser le service en essayant de contacter directement les techniciens. Mais cette situation peut aussi naître au sein du personnel informatique qui décide d'ignorer le processus et de continuer à agir comme auparavant.

Un contrat de service (SLA) non exprimé, traduit un manque de clarté dans l'expression des besoins.

Le manque d'engagement de la direction entraîne souvent un manque de moyen (ressources humaines, formation, outils). Ce manque se traduit invariablement par un niveau insuffisant de la capacité du processus.

Il existe encore des entreprises dont le seul outil informatique de gestion des services informatiques est une feuille de calcul. Dans le cas d'une PME,

cela peut éventuellement suffire, mais en réalité, ce type de solution n'est pas suffisant, car il ne fait que calquer une organisation de type formulaire papier et n'apporte pas les fonctions indispensables comme la gestion des configurations, la gestion des connaissances ou autre. Évidemment, il faut éviter d'équiper une petite structure d'un logiciel et d'un matériel hors de coût, car cela rendrait difficile la justification du retour sur investissement. Cependant, un minimum « vital » est indispensable.

Outils

Le processus de gestion des incidents étant très fortement lié au centre de services, ses outils le sont également. L'application de gestion du centre de services est utilisée comme point de départ à toutes les interventions nécessaires à la résolution des incidents. Pour s'assurer de l'efficacité du processus, on peut simplement mettre l'accent sur certains points.

Un premier type d'outil simple à mettre en place concerne l'escalade automatique qui doit s'activer en fonction d'un délai au-delà duquel l'équipe n'a pas apporté de réponse.

La détection automatique d'incident et l'envoi d'alertes concernant les ordinateurs, réseaux, applications et services du système d'information, sont également très efficaces, puisqu'ils permettent d'être averti d'un problème très rapidement, et au moins en même temps que l'utilisateur.

La recherche et l'extraction des données de la base de connaissances et de configurations CMDB doivent être systématiquement réalisées vers la fiche d'incident, afin d'apporter le plus d'information au technicien.

Enfin, l'accès banalisé et rapide à l'application de gestion des incidents (exemple : accès client Web/intranet) permet au technicien de remplir ses rapports d'intervention immédiatement, et d'accéder à sa file d'attente d'incidents sans avoir à revenir à son bureau.

Rôles et responsabilités

Responsable

Dans la plupart des entreprises, le responsable de la gestion des incidents est très logiquement le responsable du centre de services. Son premier rôle est de gérer l'équipe technique et en particulier la répartition des tâches au sein de cette équipe. Il doit également mesurer l'efficacité de son organisation et proposer des améliorations. Enfin il doit concevoir et produire les rapports destinés à la direction et aux utilisateurs.

D'un point de vue compétences, il s'agit là d'une personne méthodique, aimant le contact humain et la gestion d'une équipe sous pression, et dotée d'un sens aigu de la diplomatie. En fonction de l'importance de

l'équipe, la compétence technique n'est pas indispensable, mais constitue un atout utile dans l'animation et le management de l'équipe.

Équipe

Les membres de l'équipe de support ont pour rôle de traiter, résoudre puis clôturer les incidents qui leurs sont soumis, le plus rapidement possible. Si l'incident n'est pas de sa compétence ou la dépasse, le technicien doit être en mesure d'identifier la personne appropriée afin de rapidement lui affecter l'incident ou, à défaut vers le niveau supérieur adapté.

Méthodique, techniquement compétent, appréciant le contact humain et sachant garder son calme, le profil du technicien de support n'est pas toujours simple à trouver. Faire l'impasse sur ce genre de recrutement n'est pas une bonne méthode pour assurer l'efficacité de la gestion des incidents. De plus, il faut garder à l'esprit que cette équipe est souvent le principal interlocuteur entre le service informatique et les utilisateurs. La perception que ces derniers ont des techniciens contribue largement à l'impression globale que donne le service informatique et par conséquent à son image auprès de la direction.