جامعة سطيف2

قسم العلوم السياسية

مقياس الأمن المؤسسي وإدارة الازمات

السنة الثالثة تنظيمات سياسية وإدارية

اعداد الدكتور/ محي الدين حداد

الموسم الجامعي/ 2025-2026

محتوى المقياس

المحور الأول: ماهية الامن المؤسسي *What Is Corporate Security?*

1-1- مفهوم أمن المؤسسات.

2-1- أركان الأمن المؤسسي.

3-1- أهمية الامن المؤسسي.

4-1- تحديات الامن المؤسسي.

5-1- الامن السيبراني والمعلوماتي

المحور الثاني: الأمن الوقائي *preventive security*

2-1-الاطر التشريعية لأمن المؤسسات

2-2-الامن الداخلي للمؤسسات

2-3-الاخطار المعرضة للمؤسسة

2-4-تحديد المسؤوليات الامنية

2-5-التخطيط الأمني.

المحور 3: مفهوم ادارة الازمات

4-1-مفهوم ادارة الازمات ومراحلها

4-2- خطوات ادارة الازمات

4-3 التنظيم في الازمات

المحور 4 / الامن المؤسسي وإدارة الأزمات والوسائط الحديثة للاتصال

5-1- التخطيط الاستراتيجي وإدارة الأزمات

5-2- أثر التخطيط الاستراتيجي في إدارة الأزمات

5-3- العلاقات العامة وإدارة الأزمات

أهداف المقياس

نسعى من خلال هذا المقياس الصول الى الأهداف التالية:

1- تمكين الطالب من التعرف على فهم الامن المؤسسي وإدارة الازمات

2- وصف المخاطر التي يمكن لأمن الشركات إدارتها

3- إكساب الطالب المعارف اللازمة حول الامن المؤسسي وإدارة الازمات

4- تعميق المفاهيم المرتبطة بإدارة الازمات

5- أهمية توظيف الامن المؤسسي في إدارة أزمات المؤسسات

مقدمة

ما هو الامن المؤسسي؟ سؤال بسيط ولكنه يحمل الكثير من التعقيدات والابعاد، فالأمن يعتبر ضرورة إنسانية ملحة ارتبطت بوجوده وبقاءه، وقد أصبح الامن سلعة تتنافس عليها الأمم والمجتمعات في بيئة ديناميكية معقدة.

تعمل الشركات اليوم في بيئة تنافسية أكثر تعقيداً وتطوراً وترابطاً مما كانت عليه قبل عشرين أو حتى عشر سنوات. يتطلب النجاح في هذه البيئة من المؤسسات اتخاذ مخاطر ذكية، والتوسع في مجالات جديدة، والاستثمار في الابتكارات، وبناء شراكات جديدة. وتلعب وظيفة أمن الشركات دوراً حاسماً في تمكين اتخاذ المخاطر الذكية من خلال توفير معلومات استخباراتية عن المخاطر وضمان سلامة وأمن أصول المؤسسة المادية وموظفيها وعملياتها في كل مشروع.

ولتحقيق الامن في المؤسسات والتقليل من حوادث العمل، اعتمدت معظم الدول سياسات تعني بتوفير ظروف عمل أمنة صحية في أماكن العمل إن ّ الأمن العام هو مصطلح ٌ يُشير إلى كل ما يتعلق بحفظ مظاهر الاستقرار والسلامة العامة في أي بلد في العالم، وينطوي تحت هذا المصطلح، سالمة المواطنين والمنشآت من اشكال الفساد الاقتصادي والتطرف، والخطر والتهديد من الجهات الخارجية.

وتهدف نظم السلامة والأمن إلى حماية كل من المنشآت والممتلكات الخاصة بالشركة والعاملين والموظفين فيها من الحوادث والإصابات المؤذية، الناتجة عن أسلوب العمل، أو عن خطأ في الإدارة والتوظيف، وتعتمد كل شركة على نظم السلامة والأمن الخاصة بها، والتي يجب أن تكون مجموعة من القواعد والأساسيات المتفق عليها مسبقاً من قبل كل من أصحاب الشركة والموظفين فيها، بحيث يطّلع عليها الطرفان قبل عقد الاتفاق بينهما.

ومن أجل تطوير استراتيجية أمنية فعالة، نحتاج إلى مواجهة المخاطر التي يتعرضون لها للعمال المناسبين. على سبيل المثال، تختلف الإجراءات الأمنية لمنشآت النفط عن إجراءات تأمين أعمال البناء. على أساس العديد من القواعد والقواعد،بما في ذلك ما هو ثابت وما هو متغير وفقاً لمتطلبات وتطورات العلوم الحديثة، يجب أن يسبق تخطيط أي عملية وقتاً كافياً، ويجب النظر فيها مع مراعاة جميع الاحتمالات

والقواعد التي تهدف إلى السلامة والصحة، والتي تضمن حماية عناصر الإنتاج الرئيسية، بما في ذلك التدابير المتخذة لمنع الحرائق والسلامة البيئية والسلامة المهنية والنفسية للعمل

مفهوم الامن المؤسسي

الأمن هو حالة من الشعور بالاطمئنان والخلو من الخوف أو التهديد، الناتجة عن مجموعة من الإجراءات والتدابير والهياكل المصممة للحماية من الأخطار.

الأبعاد المختلفة لمفهوم الأمن

1. الأمن بمفهومه الشامل (العام)

هو حالة من الاستقرار والطمأنينة التي تسمح للأفراد والجماعات والدول بممارسة حياتهم وأنشطتهم دون خوف على أنفسهم أو ممتلكاتهم أو قيمهم من أية تهديدات خارجية أو داخلية. وهو يشمل:

- **الأمن الفردي** :حريات الإنسان وحقوقه الأساسية.
- **الأمن المجتمعي** :تماسك المجتمعات وهوية الثقافات.
- **الأمن الوطني** :سيادة الدولة واستقرارها السياسي والاقتصادي.
- **الأمن الدولي** :السلام والاستقرار في العلاقات بين الدول.

2. الأمن الوطني(National Security)

هو قدرة الدولة على حماية حدودها، ومواطنيها، ومصالحها الحيانية، وقيمها من التهديدات العسكرية والسياسية والاقتصادية. أدواته تشمل:

- **القوات المسلحة**)الجيش.(
- **الدبلوماسية.**
- **الاستخبارات.**
- **القوة الاقتصادية.**

3. الأمن السيبراني (Cybersecurity)

هو حماية الأنظمة والشبكات والبيانات من الهجمات الرقمية. يهدف إلى تقليل خطر الهجمات الإلكترونية والحماية من الاستغلال غير المصرح به للأنظمة والشبكات والتقنيات. مجالاته تشمل:

- أمن الشبكات.
- أمن التطبيقات.
- أمن المعلومات.
- أمن العمليات.

4. أمن المعلومات (Information Security)

هو علم وممارسة حماية المعلومات من الوصول، أو الاستخدام، أو الكشف، أو الانقطاع، أو التعديل، أو الإتلاف غير المصرح به. يقوم على ثلاثة مبادئ أساسية تُعرف بـ "ثالوث أمن المعلومات:(CIA Triad) "

- **السرية :(Confidentiality)** ضمان أن المعلومات لا تُكشف إلا للأشخاص المصرح لهم.
- **السلامة :(Integrity)** ضمان دقة واكتمال المعلومات وعدم تعديلها بطرق غير مشروعة.
- **التوافر :(Availability)** ضمان إمكانية الوصول إلى المعلومات والأنظمة عند الحاجة إليها من قبل المستخدمين المصرح لهم.

5. الأمن الفكري (Intellectual Security)

هو حماية الأفكار والمبادئ والمعتقدات من التلاعب أو الغزو أو التشويه، والحفاظ على الهوية الثقافية والفكرية للمجتمع.

6. الأمن الاقتصادي (Economic Security)

هو قدرة الفرد أو المجتمع أو الدولة على تلبية احتياجاته الاقتصادية الأساسية والحفاظ على استقراره المالي والاقتصادي في وجه التحديات والتقلبات.

7. الأمن الاجتماعي(Social Security)

هو مجموعة من البرامج والحماية التي توفرها الدولة لمواطنيها لضمان مستوى معيشي لائق، والوقاية من المخاطر مثل البطالة، المرض، العجز، الشيخوخة، وغيرها.

الخلاصة

الأمن ليس مفهوماً سلبياً (مجرد انعدام التهديد) بل هو مفهوم **ديناميكي واستباقي** .إنه عملية مستمرة تتطلب:

- **التقييم المستمر** للمخاطر.
- **وضع التدابير الوقائية.**
- **الاستعداد للاستجابة** للحوادث عند وقوعها.
- **التكيف** مع التهديدات المتطورة.

في أبسط صوره، **الأمن هو الأساس الذي يُبنى عليه الاستقرار، والنمو، والازدهار** على جميع المستويات، بدءاً من الفرد ووصولاً إلى المجتمع والدولة.

ما هو أمن الشركات؟

تستخدم وظيفة أمن الشركات الأفراد والعمليات والتكنولوجيا لحماية المؤسسة من الأحداث والمواقف السلبية. يحدد أمن الشركات التهديدات الداخلية والخارجية التي تهدد موظفي المؤسسة وممتلكاتها وأصولها، ويراقبها، ويمنعها، ويدير الأزمات المادية عند حدوثها. كما يُقيّم المخاطر التي تتعرض لها المؤسسة، ويُبلغ بها المديرين التنفيذيين والإدارة، ويُديرها على النحو المناسب.

ليس من غير المألوف أن تُشارك بعض مسؤوليات وظيفة أمن الشركات مع إدارات أخرى. على سبيل المثال، بينما تندرج مخاطر المعلومات والأصول الرقمية ضمن مظلة أمن الشركات في بعض المؤسسات، إلا أنها غالباً ما تُدار من قِبل إدارات منفصلة ولكنها ذات صلة بالأمن السيبراني أو أمن المعلومات

داخل الشركة. وبالمثل، بينما تندرج استمرارية الأعمال والمرونة غالباً ضمن أمن الشركات، إلا أنهما قد توجدان في بعض المؤسسات بشكل منفصل عن وظيفة أمن الشركات، ولكن بالشراكة معها.

فالأمن عنصرٌ أساسيٌّ في خدماتنا ومفتاح نجاح الشركة. جميع أفراد المؤسسة مسؤولون عن اتخاذ الاحتياطات اللازمة لحماية الشحنات والأصول الموكلة إلينا. لذلك، يجب علينا تهيئة بيئة آمنة يثق بها عملاؤنا.

المخاطر على الأفراد :يحتاج الموظفون والمديرون التنفيذيون ويستحقون أماكن عمل آمنة ومأمونة. يمكن لأمن الشركات التعاون مع الموارد البشرية لتوفير التدريب والخدمات التي تتوقع حوادث العنف في مكان العمل وتردعها، ويمكنها نشر الموظفين والتكنولوجيا لإبعاد الأفراد غير المصرح لهم عن حرم الشركة. يمكنهم وضع ضوابط للتخفيف من حدة المخاطر بجميع أنواعها - من الكوارث الطبيعية إلى المظاهرات وأعمال الشغب - وتنفيذ شبكات اتصال للموظفين وفرق الاستجابة الأولية. في حال وقوع مثل هذه الحوادث، يُمكن لأمن الشركات الحفاظ على التواصل مع الموظفين والعاملين لتوجيه الاستجابة للطوارئ. يمكن لأمن الشركات توفير خدمات حماية الأفراد، والحفاظ على سلامة الموظفين المعرضين للخطر في العمل، وعلى الطرق، وغالباً في المنزل أيضاً.

مخاطر الممتلكات والأصول .تأتي التهديدات لأصول الشركة بأشكال وزوايا متعددة. يمكن لأمن الشركات استخدام تقنيات وعمليات منع الخسائر لمنع سرقة الأصول من داخل المؤسسة وخارجها. يمكنهم أيضاً رصد وتوقع التهديدات للملكية الفكرية القيّمة. يمكن لأمن الشركات حماية المواقع التقليدية، مثل المكاتب ومواقع التصنيع، من الأضرار المتعمدة. يمكنهم أيضاً تأمين المنتجات والمواد على طول سلسلة التوريد.

مخاطر الاستمرارية .يحافظ أمن الشركات على استمرارية العمل عند حدوث أي طارئ. يضعون ويطبقون ويراجعون خطط إدارة الأزمات لضمان توفر خدمات احتياطية في حال حدوث أي عطل. يدير أمن الشركات مراكز عمليات إقليمية أو عالمية يمكنهم من خلالها مراقبة الحوادث والاستجابة لها، وجمع المعلومات الاستخبارية، والتواصل مع أصحاب المصلحة. يعمل الأمن مع الشركاء الداخليين

والخارجيين، بما في ذلك الحكومات وخدمات الطوارئ، بعد وقوع حادث لتحديد الدروس التي يمكن تعلمها وتطبيقها في الأزمة التالية.

مخاطر أعمال أخرى. غالباً ما يُجري قسم أمن الشركات تقييمات وتحليلات للمخاطر لفهم المخاطر التي قد تؤثر بشكل كبير على استراتيجية العمل وعملياته. وبناءً على النتائج، يُمكن للأمن تطوير استراتيجيات التخفيف المناسبة. إن توثيق السياسات والإجراءات التي يُنشئها قسم أمن الشركات يُمكن أن يحمي الشركات من التقاضي، كما تُساعد قدراته الاستخباراتية في التخفيف من مخاطر السمعة التي قد تُهدد المؤسسة.

لأمن المؤسسي هو إطار عمل متكامل وسلسلة من الممارسات والاستراتيجيات التي تتبناها المؤسسة لحماية جميع أصولها من التهديدات الداخلية والخارجية، لضمان استمرارية العمل وتحقيق الأهداف الاستراتيجيةstop.

لا يقتصر الأمن المؤسسي على حماية المبنى físico أو الأجهزة فقط، بل يشمل حماية كل ما له قيمة للمؤسسة، وهو **نهج استباقي وشامل** يتجاوز مفهوم "الأمن التقليدي" المتمثل في الحراس والكاميرات.

ولطالما اعتمدت المؤسسات على وظيفة أمنية لحماية أصولها الحيوية. ومع مرور الوقت، شهدت وظيفة أمن المؤسسات، تحولاً جذرياً، من نموذج "الحراسة والحماية والبوابات" التقليدي إلى نموذج يشمل التهديدات الأمنية التي تتجاوز الجوانب المادية البحتة، وتتداخل مع تخصصات أخرى مثل "الأمن السيبراني". ونظراً لأن عمل الأمن المؤسسي يتضمن التخفيف من المخاطر الأمنية بشكل استباقي وتجنب التهديدات.

وفي ظل تزايد حالة عدم اليقين وعدم الاستقرار، تحول التركيز مجدداً إلى الدور المستقبلي لأمن المؤسسات. ومع مواجهة المؤسسات لمجموعة متزايدة من التهديدات المستقبلية المحتملة، يدفع هذا إلى إعادة النظر في كيفية تكيف أمن المؤسسات مع السياق الجديد. كما تشير حوكمة الأمن إلى كيفية تحكم

المؤسسة وتوجيه نهجها الأمني. عند تطبيقها بفعالية، تُوفر حوكمة الأمن مساراً لتوجيه المؤسسة في أنشطتها المتعلقة بالأمن، مما يُسهم في إثراء عملية صنع القرار، ويُرسي خطوط اتصال ومساءلة واضحة.

يرتبط مفهوم الأمن في أماكن العمل بإنتاجية العاملين وأدائهم بسبب ارتياحهم في العمل وتمتعهم بالطمأنينة والسلامة اللازمة لأداء مهامهم، لذا استوجب الاهتمام بسالمة العنصر البشري في المؤسسات، الن هذا المورد هو أحد متطلبات قيام المنظمات والمؤسسات وأساس نجاحها ويتطلب ذلك توفير بيئة العمل السليمة والإمكانات الصحية المطلوبة لحماية هذا المورد الحيوي وجعله يتمتع بكل مقومات الكفاءة والفعالية من جهة والحفاظ على إنتاجية العاملين من جهة أخرى.

تعريف الأمن في أماكن العمل :

هو عبارة عن إجراءات تهدف إلى حماية مختلف فئات العمال، من التأثيرات الصحية الخطيرة الفورية أو البعيدة المدى، من خلال معالجة المصادر الشخصية، التقنية والبيئة المؤدية إلى هذه المخاطر، بشكل يسمح للعمال التمتع بصحة بدنية، نفسية واجتماعية مناسبة.

أما بمفهومه البسيط فيعني: «توفير بيئة عمل آمنة وصحية، للحفاظ على ثالثة من المقومات الأساسية لعناصر الإنتاج: الإنسان، الآلة، والمادة، ضمن خلق جو من السالمة والطمأنينة، لحماية العنصر البشري من الحوادث والأمراض المهنية، وفي الوقت نفسه الحفاظ على عناصر الإنتاج الأخرى من احتمالات التلف والضياع وبالتالي تخفيض تكاليفها والرفع من كفايتها الإنتاجية.

وقد عرفت منظمة العمل الدولية الأمن في العمل: "يهدف إلى العمل والمحافظة على تحقيق أعلى درجة من الصحة البدنية والعقلية، والرفاه الاجتماعي للعمال في جميع المهن".

يمكن أن نستخلص من التعريفات السابقة أن الأمن والسلامة في أماكن العمل مجال يهدف إلى حماية العنصر البشري بالدرجة الأولى، إلا أن مهمته تتعدى ذلك، إلى حماية بقية عناصر الإنتاج من مختلف الأضرار ويعمل على البحث عن الأسباب الحقيقية لحوادث العمل، والأمراض المهنية من مصادرها الإنسانية والمادية، والعمل على معالجتها ومنع تكرارها، كما انه مجال ال يقتصر على المؤسسات الصناعية فحسب، بل يهتم بجميع أنواع المؤسسات

1. ما هي "الأصول" التي يحميها الأمن المؤسسي؟

- **الأصول المادية** materiel: المباني، المركبات، المعدات، الأثاث.
- **الأصول البشرية** : الموظفون، العملاء، المدراء.
- **الأصول المعلوماتية** : البيانات (ملفات العملاء، الأسرار التجارية، الخطط الاستراتيجية)، قواعد البيانات، الحقوق الفكرية.
- **الأصول المالية** : الأموال، الأسهم، الاستثمارات.
- **الأصول غير الملموسة** : السمعة التجارية، صورة العلامة التجارية، ثقة العملاء.

2. ما هي التهديدات التي يواجهها؟

- **التهديدات المادية** : السرقة، التخريب، الاعتداء، الحرائق، الكوارث الطبيعية.
- **التهديدات السيبرانية** : هجمات القرصنة، برامج الفدية، اختراق البيانات، التصيد الاحتيالي.
- **التهديدات البشرية** : أخطاء الموظفين (عن غير قصد)، سوء الاستخدام الداخلي، أعمال التخريب من الداخل، تجسس الموظفين.
- **التهديدات التشغيلية** : انقطاع التيار الكهربائي، فشل الشبكة، أخطاء في الإجراءات.
- **تهديدات السمعة** : الشائعات، الأخبار السلبية، أزمات العلاقات العامة.

2- اركان الامن المؤسسيstop

أركان الأمن المؤسسي.(Cybersecurity Framework Pillars)

الأمن المؤسسي ليس مجرد برنامج مكافحة فيروسات أو جدار حماية، بل هو نظام متكامل مبني على عدة أركان أساسية تتعاون معًا لحماية أصول المؤسسة المعلوماتية (البيانات، الأنظمة، الشبكات، الأجهزة) من التهديدات الداخلية والخارجية.

عادةً ما تُصنف هذه الأركان إلى خمسة أساسية، وغالبًا ما يتم تمثيلها في إطار عمل مشهور مثل إطار NIST(المعهد الوطني للمعايير والتقنية في الولايات المتحدة

National Institute of Standards and Technology

). هذه الأركان الخمسة هي:

1. التحديد(Identify)
2. الحماية(Protect)
3. الكشف(Detect)

4. **الاستجابة(Respond)**
5. **الاسترداد(Recover)**

1.ركن التحديد(Identify)

الهدف :فهم البيئة المؤسسية بشكل كامل لتحديد الأصول التي تحتاج للحماية والمخاطر التي تهددها. هذا هو أساس جميع القرارات الأمنية.

الأنشطة الرئيسية:

- **إدارة الأصول :حصر وجرد جميع الأصول التقنية (خوادم، أجهزة، برامج) وغير التقنية (بيانات، موظفون، سمعة).**
- **إدارة المخاطر :تحديد وتقييم وتحليل المخاطر الأمنية المحتملة وتأثيرها على العمل.**
- **الحوكمة :وضع السياسات والإجراءات والإستراتيجيات الأمنية التي تتبعها المؤسسة.**
- **تحديد البيئة التشغيلية :فهم كيفية سير العمل وكيفية تفاعل الأصول مع بعضها البعض.**

مثال :إنشاء سجل لكل أجهزة الشركة، وتحديد أن قاعدة بيانات العملاء هي "أكثر الأصول حساسية"، وتحليل خطر تعرضها لاختراق.

2.ركن الحماية(Protect)

الهدف :تنفيذ الضوابط اللازمة لتقليل احتمالية وقوع الهجمات أو الحد من تأثيرها.

الأنشطة الرئيسية:

- **التحكم في الوصول :ضمان منح صلاحيات الوصول إلى البيانات والأنظمة للمستخدمين المصرح لهم فقط (كلمات مرور قوية، المصادقة متعددة العوامل).**
- **التوعية الأمنية :تدريب الموظفين على الممارسات الآمنة وكيفية التعرف على محاولات التصيد.**
- **أمن البيانات :تشفير البيانات المخزنة والمنقولة.**
- **الصيانة الوقائية :تحديث الأنظمة والبرامج باستمرار (إدارة التصحيحات).**
- **التأمين التقني :استخدام الحلول التقنية مثل جدران الحماية(Firewalls) ، وبرامج مكافحة الفيروسات.**

مثال :تطبيق سياسة كلمات مرور معقدة، وتشفير أقراص الأجهزة المحمولة، وتدريب الموظفين على عدم فتح مرفقات البريد الإلكتروني المشبوهة.

3.ركن الكشف(Detect)

الهدف :اكتشاف الحوادث الأمنية بشكل سريع وفعال عند حدوثها. لا يمكنك منع كل هجوم، ولكن يجب أن تكتشفه بأسرع ما يمكن.

الأنشطة الرئيسية:

- **المراقبة المستمرة :**استخدام أنظمة كشف التسلل (IDS) ومراقبة حركة المرور على الشبكة.
- **إدارة السجلات والتحليل :**جمع وتحليل سجلات الأحداث (Logs) من الأنظمة والتطبيقات للعثور على أنشطة غير طبيعية.
- **اختبارات الكشف :**إجراء اختبارات اختراق وتمارين دورية للتأكد من فعالية أنظمة الكشف.

مثال :وجود نظام لمراقبة الشبكة ينبه فريق الأمن عند محاولة دخول غير عادية إلى الخادم في منتصف الليل، أو اكتشاف برنامج ضار يحاول الاتصال بخادم خارجي.

4.ركن الاستجابة(Respond)

الهدف :احتواء الحادث الأمني والتخفيف من آثاره عند اكتشافه.

الأنشطة الرئيسية:

- **التخطيط للاستجابة :**وجود خطة استجابة للحوادث واضحة ومحددة الأدوار.
- **الاحتواء :**عزل الأنظمة المتأثرة لمنع انتشار الهجوم (مثل فصل الجهاز المصاب عن الشبكة).
- **التحقيق :**تحليل سبب الحادث وكيفية حدوثه وتحديد حجم الضرر.
- **الإبلاغ :**إخطار الجهات المعنية داخلياً (الإدارة) وخارجياً (إذا تطلب الأمر قانونياً).
- **القضاء :**إزالة سبب الحادث (مثل حذف البرنامج الضار).

مثال :عند اكتشاف هجوم تصيد ناجح، يقوم الفوراً بتعطيل حساب الموظف المتأثر، وتغيير كلمات المرور، وفحص الجهاز للتأكد من خلوّه من البرمجيات الخبيثة.

5.ركن الاسترداد(Recover)

الهدف :استعادة القدرات التشغيلية والخدمات التي تأثرت بالحادث الأمني والعودة إلى العمل الطبيعي في أسرع وقت ممكن.

الأنشطة الرئيسية:

- **التخطيط للاسترداد :**وجود خطة استعادة الكوارث (Disaster Recovery Plan) وخطط استئناف العمل.(Business Continuity Plan)
- **استعادة الأنظمة والبيانات :**استخدام النسخ الاحتياطية (Backups) لاستعادة البيانات والأنظمة المفقودة أو التالفة.
- **تحسين الإجراءات :**التعلم من الحادث وتحديث السياسات والإجراءات والأدوات لمنع تكرار الحادث مستقبلاً.
- **التواصل :**إبقاء جميع أصحاب المصلحة (عملاء، موظفين) على علم بحالة الاسترداد.

مثال :بعد هجوم الفدية، تقوم المؤسسة بمسح الأنظمة المصابة تماماً وإعادة بنائها، ثم استعادة البيانات من آخر نسخة احتياطية نظيفة، وأخيراً مراجعة ثغرات الأمان التي سمحت بحدوث الهجوم.

خلاصة

هذه الأركان الخمسة لا تعمل بمعزل عن بعضها، بل هي **دورة حياة مستمرة ومترابطة** .تبدأ بفهم بيئتك (تحديد)، ثم تحميها (حماية)، وعندما تفشل الحماية تقوم بالكشف عن المشكلة (كشف)، ثم تتعامل معها (استجابة)، وأخيراً تعود إلى وضعك الطبيعي وتتعلم من التجربة (استرداد)، ثم تعيد التحديد بناءً على الدروس المستفادة، وهكذا.

بناء نظام أمني مؤسسي قائم على هذه الأركان هو الضمانة الأفضل لحماية المؤسسة في عالم رقمي مليء بالتهديدات المتطورة.

2-1- <u>أهمية الامن المؤسسي.</u>

التكنولوجيا: تُعدّ التكنولوجيا عاملاً أساسياً يجب مراعاته في مجال الأمن السيبراني في أي مؤسسة، فهي أدوات الأمن التي تهدف إلى حماية الشبكة من الهجمات السيبرانية. وتُعد حماية أجهزة نقاط النهاية، مثل الحواسيب والأجهزة الذكية وأجهزة التوجيه والشبكات والسحابة، أمراً أساسياً، باستخدام جدار الحماية، وبرامج الحماية من البرامج الضارة، ومكافحة الفيروسات،، وحلول التصيد الاحتيالي عبر البريد الإلكتروني.

الأفراد: يجب على الأفراد أو الموظفين فهم القضايا الحرجة المتعلقة بالهجمات الإلكترونية، ولحماية أنفسهم، يجب استخدام كلمات مرور قوية، وعدم فتح أي مرفقات مشبوهة في البريد الإلكتروني، وضغط الملفات أو المستندات دائماً عند إرسالها عبر البريد الإلكتروني، وحفظ كلمة مرور النظام أو أي كلمة مرور أخرى في أماكن آمنة، وعدم فتح أي موقع مشبوه. كما يجب عدم ترك أي شخص أي أجهزة مثل الكمبيوتر المحمول أو الكمبيوتر دون مراقبة، وتوخي الحذر الشديد عند فتح أي مرفق في البريد

الإلكتروني، وتصفح أي موقع عبر شبكة Wi-Fi أو الإنترنت الآمنة، ونسخ البيانات احتياطياً بانتظام، وغيرها من أهم نصائح الأمن السيبراني للمستخدمين.

العمليات: لكل مؤسسة بعض العمليات المُعدّة للتعامل مع الهجمات الإلكترونية. سيساعد وجود هيكل دعم أساسي في كيفية التعرف على الهجمات الإلكترونية، وحماية الشبكة والأنظمة، ورصد التهديدات والتصدي لها، والتعافي من الهجمات الناجحة. يمكن تحديد أفضل ممارسات الأمن السيبراني للتغلب على التهديدات، والتي ستتضمن معلومات محددة حول ضوابط الأمان (مثل إدراج عناوين IP في القائمة البيضاء، والوصول إلى جدار الحماية، وما إلى ذلك). يمكن إعداد صناديق فحص الثغرات الأمنية باستخدام أحدث البرامج لفحص كل نظام دورياً ومراقبة حركة البيانات.

تحديد المسؤوليات الأمنية

تنقسم الى 3 اقسام:

1- **المسؤولية الاشرافية: يتولاها مدير/ رئيس المؤسسة الذي تصدر جميع الأوامر باسمه، ومن مهامه اصدار الأوامر لتحديد المسؤوليات والاشراف على تنفيذ الإجراءات الأمنية، القيام بالمراقبة الدورية والمفاجئة، الإبلاغ عن أي خطر او حادث يسمن بأمن المؤسسة**

2- **المسؤولية التنفيذية يقوم بها أعوان الامن ورؤساؤهم ومن مهامهم: وضع القواعد الأمنية اللازمة- اختيار الافراد المساعدين وتدريبهم-القيام بمهام التحري عن المخاطر والتهديدات-اتخاذ إجراءات الامن للأفراد والممتلكات والاتصالات**

- **مواجهة الشائعات الهدامة**
- **وضع خطة تامين ضد المخاطر-مخطط دفاع-**

- **المسؤولية الافتراضية: يتولاها جميع العاملين في المؤسسة**

أهمية السياسات الأمنية في المؤسسات

إن وجود سياسات أمنية فعالة يعد أمراً حيوياً لضمان سلامة المعلومات والموارد، وحماية سمعة المؤسسة. تساعد السياسات الأمنية في وضع إطار عمل واضح يحدد كيفية التعامل مع المخاطر المحتملة. تستهدف توفير توجيهات وإجراءات محددة يجب اتباعها من قبل جميع الموظفين، مما يعزز من الوعي الأمني داخل المؤسسة.

بالإضافة إلى ذلك، فإن السياسات الأمنية تعكس التزام الإدارة العليا بحماية الأصول والمعلومات، مما يعزز الثقة بين الموظفين والعملاء والمستثمرين.

أهمية تطبيق السياسات الأمنية في المؤسسات

تطبيق السياسات الأمنية بشكل فعال يعد أمراً حيوياً لضمان تحقيق الأهداف المحددة. فعندما يتم تنفيذ السياسات بشكل صحيح، يمكن للمؤسسات تقليل المخاطر المرتبطة بالتهديدات الأمنية بشكل كبير. على سبيل المثال، يمكن أن يؤدي تطبيق إجراءات التحكم في الوصول إلى تقليل فرص الوصول غير المصرح به إلى المعلومات الحساسة.

بالإضافة إلى ذلك، فإن تطبيق السياسات الأمنية يعزز من ثقافة الأمان داخل المؤسسة. عندما يشعر الموظفون بأن هناك نظاماً أمنياً قوياً قائماً، فإنهم يكونون أكثر وعياً بمسؤولياتهم تجاه حماية المعلومات. هذا الوعي يمكن أن يؤدي إلى سلوكيات أكثر أماناً ويقلل من الأخطاء البشرية التي قد تؤدي إلى حوادث أمنية

5-التعريف بالأمن السيبراني

الأمن السيبراني مفهوم معقد يحمل الكثير من المعاني والتعريفات، ورغم اختلافها فإنها تتفق على وظيفته العامة تقريبا.

يعرف بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنية الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن.

وحسب الاتحاد الدولي للاتصالات **فالأمن السيبراني** هو "مجموعة من الأدوات والسياسات والمفاهيم الأمنية والتحفظات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب، وغيرها من الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المؤسسات والمستعملين من المخاطر الأمنية ذات الصلة في البيئة السيبرانية."

وتعرفه وكالة الأمن السيبراني وأمن البنية التحتية الأميركية (سي آي إس إيه) بأنه "فن حماية الشبكات والأجهزة والبيانات من الوصول غير المصرح به أو الاستخدام الإجرامي، ويمثل ممارسة ضمان سرية المعلومات وسلامتها وتوافرها."

وتعرفه الموسوعة البريطانية بأنه "حماية نظم الحوسبة والمعلومات من الأضرار والسرقة والاستخدام غير المصرح به."

وتعرفه شركة "كاسبر سكاي" الدولية الخاصة للأمن السيبراني بأنه "أشكال الدفاع عن الحواسيب والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الخبيثة، ويعرف أيضا بأمن تكنولوجيا المعلومات أو الأمن الإلكتروني للمعلومات"

بالنسبة للمشرع الجزائري: الامن السيبراني يمثل مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة.

الأمن السيبراني للمؤسسات

يحمي الأمن السيبراني للمؤسسات تطبيقات الشركة وبياناتها وبنيتها التحتية من التهديدات الإلكترونية. فهو يحمي الشبكات المحلية وأصول السحابة والأجهزة البعيدة، ويهدف إلى تعزيز أمن المؤسسة من خلال مواجهة الجهات الخبيثة. وبذلك، يُقلل من مخاطر اختراق البيانات.

ما هو الأمن السيبراني للمؤسسات؟

الأمن السيبراني للمؤسسات هو نهج متكامل يركز على تقليل نقاط الضعف، وتعزيز الأنظمة ضد التهديدات المعروفة، وضمان استمرارية العمليات حتى في حال نجاح الهجمات.

يتضمن الأمن السيبراني للمؤسسات تطبيق ضوابط أمنية متعددة الطبقات عبر الشبكات ونقاط النهاية والتطبيقات والبيانات لمواجهة مجموعة واسعة من المخاطر السيبرانية التي تواجه المؤسسات الكبيرة. وتستفيد استراتيجية الأمن السيبراني الفعّالة للمؤسسات من أحدث الحلول التكنولوجية، بالإضافة إلى السياسات والتدريب، لتطوير وضع أمني قوي.

تعتمد المؤسسات على متخصصي الأمن السيبراني لتنفيذ إستراتيجيات الحماية. ويقيم هؤلاء الخبراء المخاطر الأمنية التي قد تواجه أنظمة الحوسبة والشبكات ومخازن البيانات والتطبيقات والأجهزة المتصلة. ثم يضعون إطارا شاملا للأمن السيبراني ويطبقون تدابير الحماية اللازمة داخل المؤسسة.

وتحرص المؤسسات على توعية الموظفين بأفضل الممارسات الأمنية، وتفعيل تقنيات الدفاع الآلي في البنية التحتية لتكنولوجيا المعلومات. بهدف تشكيل طبقات من الحماية ضد التهديدات المحتملة، مما يساعدها في تحديد المخاطر المتوقعة، وحماية الهويات والبيانات والبنية التحتية، ومراقبة الأعطال ورصدها، والاستجابة السريعة وتحليل أسبابها، والأهم التعافي بعد وقوع الهجمات.

وتعتمد مؤسسات الأمن السيبراني عدة مبادئ أساسية في عملها، الأول مبدأ "انعدام الثقة"، الذي يتطلب مصادقة صارمة ومراقبة مستمرة لجميع المستخدمين والتطبيقات. الثاني تحليلات السلوك لمراقبة الأنشطة غير المعتادة في نقل البيانات والتنبيه بشأنها.

المحور الثاني: ادارة الازمات في المؤسسة

مفهوم الازمة

مصطلح الأزمة من بين المصطلحات الشائعة لدى كل المتجمعات الإنسانية منذ القدم إلى يومنا هذا ، وقد أصبحت أكثر انتشارا في المتجمعات المعاصرة ، حيث أضحت الأزمات تشكل التهديد الأكبر على حياة الأفراد والمتجمعات وكذا الدول و المؤسسات.

تحدث الأزمة نتيجة لتراكم مجموعة من التأثيرات التى تحدث خلل مفاجئ يؤثر على المقومات الرئيسية للنظام ويشـــكل تهديد لبقاء المنظمة ويؤثر على القواعد والمعايير المتبعه ويؤدى إلى اختلاط الأســـباب بالنتائج وبالتالى يفقد صانع القرار السيطرة على الموقف .

ولا يوجد اتفاق موحد على تعريف الأزمة حيث تعددت التعريفات بتعدد وجهات النظر ونواحى الاهتمام والتركيز . وفيما يلى استعراض لبعض التعريفات الخاصة بمصطلح الأزمة

- **عرف (Mitroff & Pauchant 1992) الأزمة بأنها حالة تمزق تؤثر على النظام كله وتهدد افتراضاته الأساسية ومعتقداته الداخلية وجوهر وجوده. "**
- **كما عرف (Bieber 1988) الأزمة بأنها نقطه تحول من أوضاع غير مستقره ويمكن أن تقود إلى نتائج غير مرغوبة إذا كانت الأطراف المعنية غير مستعدة أو غير قادرة على احتوائها ودرء أخطارها .**
- **وعرف (Pauchant & Douville 1993) الأزمات بأنها مواقف مركبه تواجه المنظمة أو النظام كله وتتحدى الافتراضات الأساسية المتعارف عليها وعادة تتطلب تلك الأزمات تصرفات وقرارات عاجلة ومستحدثه وتؤدى فيما بعد لاستجواب دقيق للنظام والافتراضات الأساسية بواسطة أعضاء النظام .**

كما عرف الحملاوى (1993) الأزمة بأنها عبارة عن خلل يؤثر ماديا على النظام كله كما أنه يهدد الافتراضات الرئيسية التى يقوم عليها هذا النظام

مفهوم إدارة الأزمة هو **فلسفة إدارية** تدرك أن المؤسسات تعمل في بيئة مليئة بالمخاطر والمفاجآت. لذلك، فإنها تتحول من ثقافة "رد الفعل" و"إطفاء الحرائق" إلى ثقافة "الاستباقية" و"المرونة"، مما يمكنها ليس فقط من النجاة من العواصف، بل والخروج منها أقوى وأكثر حكمة.

ادارة الأزمة هي عملية منهجية ومخططة تستعد بها المؤسسة للتعامل مع حدث مفاجئ وغير متوقع يهدد وجودها، سمعتها، عملياتها، أو أصحاب المصلحة فيها. ببساطة، هي **فن تحويل التهديد إلى فرصة**،أو على الأقل، تقليل الآثار السلبية إلى أدنى حد ممكن.

ادارة الأزمات: هي عملية الاستعداد والاستجابة للطوارئ أو التهديدات غير المتوقعة التي يمكن أن تضر بالمنظمة وموظفيها، سمعتها، وعملائها. الهدف هو تقليل الضرر والاستعادة بأسرع ما يمكن.

الأزمة ليست مجرد مشكلة عابرة؛ فهي حدث مفاجئ أو تهديد يهدد الاستقرار، السمعة، أو الربحية، ويتطلب اتخاذ قرارات سريعة وحاسمة

- **عرف غريب عبد الحميد (1997) إدارة الأزمات بأنها كافة الوسائل والإجراءات والأنشطة التى تنفذها المنظمة بصفة مستمرة فى مراحل ماقبل الأزمة وأثنائها وبعد وقوعها والتى تهدف من خلالها إلى تحقيق مايلى :**

- **منع وقوع الأزمة كلما أمكن .**
- **مواجهة الأزمة بكفاءه وفعالية .**
- **تقليل الخسائر فى الأرواح والممتلكات إلى أقل حد ممكن .**
- **تخفيض الآثار السلبية على البيئة المحيطه .**
- **إزالة الآثار السلبية التى تخلفها الأزمة لدى العاملين والجمهور .**
- **تحليل الأزمة والاستفادة منها فى منع وقوع الأزمات المشابهه أو تحسين وتطوير قدرات المنظمة وأدائها فور مواجهة تلك الأزمات.**
- **عرف Cigliotti & Jason (1991) إدارة الأزمات بأنها (قدرة المنظمة على التعامل مع المواقف الطارئه بسرــعه وفعالية وكفاءة بهدف تقليل التهديدات والخســائر فى الأرواح والممتلكات والآثار السلبية على استمرار أنشطتها وعملياتها.)**

خصائص ادارة الازمة

- **عملية استباقية وليست رد فعل:** جوهر المفهوم هو التخطيط والاستعداد قبل وقوع الأزمة. المؤسسات الذكية لا تنتظر حدوث الكارثة، بل تتنبأ بالسيناريوهات المحتملة وتجهز خططًا لها

- . **عملية مستمرة وشاملة:** لا تنتهي بإخماد اثار الأزمة، بل هي دورة متكاملة تبدأ **بالوقاية** ثم **الاستعداد** ثم **الاستجابة** ثم التعافي والتعلم من الدروس.

- – **تركز على حماية السمعة**: أحد أهم أهداف إدارة الأزمات هو **حفظ رأس المال غير الملموس** للمؤسسة، وهو سمعتها وثقة عملائها. قد تكون الخسارة المالية مؤقتة، ولكن تدمير السمعة قد يكون دائمًا.

الاتصال هو العمود الفقري: المفهوم يركز على كيف تتحدث المؤسسة أثناء الأزمة لا يقل أهمية عما تفعله.

- **فريق عمل متخصص**: إدارة الأزمة ليست مسؤولية فرد واحد. تتطلب **فريقًا متعدد التخصصات** من الإدارة العليا، العلاقات العامة، القانونية، الموارد البشرية، والتقنية.

- **الصدق والشفافية.**
- **تحديد متحدث رسمي** واحد.
- **سرعة إيصال المعلومة** الصحيحة قبل انتشار الشائعات.

- **الفرق بين الازمة والمشكلة العادية**

الازمة	المشكلة العادية
مفاجئة وغير متوقعة إلى حد كبير.	يمكن توقعها والتعامل معها ضمن الإجراءات الروتينية.
عالية الخطورة وتهدد المصالح الحيوية للمؤسسة	تكون عادة محدودة الأثر والنتائج.
تتطلب **رد فعل سريع** وحاسماً تحت ضغط الوقت.	يتوفر وقت كافٍ لاتخاذ القرار.
تتصدر **الاهتمام الإعلامي** والجماهيري.	لا تجذب اهتمام الرأي العام بشكل كبير.

الأهداف الاستراتيجية لمفهوم إدارة الأزمة

1. **الاحتواء والسيطرة :**منع توسع نطاق الأزمة وانتشار آثارها.
2. **استمرارية الأعمال :**ضمان استئناف العمليات الحيوية في أسرع وقت ممكن.

3. **حماية الأرواح والممتلكات :**وهي الأولوية القصوى دائمًا.
4. **حماية السمعة والعلامة التجارية.**
5. **التعلم والتطوير :**استخلاص الدروس لتحسين الأداء في المستقبل.

إدارة الأزمة = الاستباقية (التخطيط) + السرعة (الاستجابة) + الشفافية (الاتصال) + التعلم (التطوير).

أهداف إدارة الأزمات :

تتمثل أهداف إدارة الأزمات فيما يلى :

1- وضع قائمة بالتهديدات والمخاطر المحتمله ووضع أولويات لها حسب أهميتها .

2- تجنب المفاجأه المصاحبه لحدوث مخاطر أو أزمات عن طريق المتابعة المستمرة والدقيقة لمصادر التهديد والمخاطر المحتملة واكتشاف إشارات الإنذار المبكر وضمان توصيلها لمتخذ القرار فى الوقت المناسب لاتخاذ إجراءات مضادة .

3- وضــع خطط الطوارئ ونظم الانذار المبكر والإجراءات الوقائية اللازمة لمحاولة منع حدوث الأزمات وتحديد خطة الاتصالات مع الأطراف المعنية وأساليب استعادة النشاط والعودة للأوضاع الطبيعية وأساليب التعلم وتحليل نواحى القوة والضعف فى عملية المنع والمواجهة لتقويم أداء الأجهزة المختلفة .

4- حسن إستغلال الوقت المتاح للمواجهة عن طريق تقليل الوقت اللازم لاتخاذ قرار المنع/ المواجهة .

5- محاولة القضاء على قدر كبير من التخبط والعشوائية وإنفعال اللحظه التى عادة ما يصاحب الأزمات .

6- الاستغلال الكفء للموارد المتاحه وضمان سرعة توجيهها للتعامل مع الأزمة .

7- القدرة على التعامل مع الأزمة بأســلوب المبادرة وليس برد الفعل والمحافظة على صــورة المنظمة أمام الأطراف المعنية والمجتمع .

8- حسن معاملة الضحايا وعائلاتهم ورفع الروح المعنوية للمتضررين .

9- استخلاص الدروس المستفادة من الأزمات السابقة وتحسين طرق مواجهتها مستقبلا .

10- أقتناص الفرص التى قد تطرحها الأزمة .

دورة حياة الأزمة :

تمر الأزمة بخمس مراحل تمثل دورة حياتها ، وتتمثل هذه المراحل فيما يلى :

1. **ميلاد الأزمة : الاحتكاك الذى يمثل الشعور بالقلق من شئ مجهول يلوح فى الأفق**
2. **نمو الأزمة : مع استمرار الاحتكاك تتراكم الآثار السلبيه ويتضخم التأثير.**
3. **نضج الأزمة:التصادم فى حالة عدم مواجهة الأزمة خلال مرحلتى الميلاد والنمو وتكون النتائج مدمره وتسبب انهيار الكيان .**
4. **انحسار الأزمة : وتمثل تدهور الأزمة بعد أن حققت أهدافها وفقدت قوة دفعها .**
5. **اختفاء الأزمة إما تكون دافعا للكيان لاســتعادة فعاليته أو تكون قد تمكنت من تدمير الكيان واختفت معه .**

مراحل إدارة الأزمات (النموذج الرباعي)

تتبع إدارة الأزمات عادة أربع مراحل رئيسية:

1.المرحلة الأولى : التخفيف والوقاية

- **الهدف :**منع حدوث الأزمة من الأساس أو تقليل احتمالية حدوثها.
- **الأنشطة:**
  - إجراء تحليل للمخاطر لتحديد التهديدات المحتملة.
  - تنفيذ برامج سلامة وأمن صارمة.
  - تدريب الموظفين على معايير الجودة والسلوك الأخلاقي.
  - تأمين البنية التحتية التكنولوجية والبيانات.

2.المرحلة الثانية: الاستعداد والتخطيط

- **الهدف :**التأهب للاستجابة بفعالية عندما تحدث الأزمة.
- **الأنشطة:**

- **وضع خطة إدارة الأزمات :**توضح أدوار ومسؤوليات فريق إدارة الأزمات، قوائم اتصال طوارئ، بروتوكولات الاتصال.
- **تشكيل فريق إدارة الأزمات :**فريق متعدد التخصصات (إدارة عليا، قانوني، علاقات عامة، موارد بشرية، تقنية معلومات).
- **تدريب فريق الأزمات وإجراء محاكاة :**لعرض الخطة واكتشاف الثغرات.
- **إعداد أدوات اتصال :**نظام للاتصال الجماعي، بيانات صحيفة جاهزة، إدارة وسائل التواصل الاجتماعي.

3.المرحلة الثالثة: الاستجابة والاحتواء

- **الهدف :**التعامل مع الأزمة فور وقوعها للسيطرة عليها وتقليل آثارها.
- **الأنشطة:**

- **تفعيل خطة إدارة الأزمات** وفريقها فورًا.
- **تقييم الموقف :**جمع المعلومات الدقيقة بسرعة لفهم نطاق الأزمة.
- **إعطاء الأولوية :**حماية الأرواح أولاً، ثم الممتلكات، ثم السمعة.
- **الاتصال الفعال) :**هذه نقطة محورية(

- **الصدق والشفافية :**الإفصاح عن المعلومات الصحيحة بسرعة.
- **التعاطف :**إظهار الاهتمام بالمتأثرين.
- **تحديد متحدث رسمي واحد :**لتجنب تضارب المعلومات.
- **استخدام جميع القنوات :**وسائل الإعلام التقليدية، مواقع التواصل الاجتماعي، الموقع الإلكتروني.

4.المرحلة الرابعة: التعافي والاستعادة

- **الهدف :**العودة إلى الوضع الطبيعي واستخلاص الدروس.
- **الأنشطة:**

- استئناف العمليات التجارية العادية.
- تقديم الدعم للمتأثرين (موظفين، عملاء).
- **إجراء تحليل لاحق للأزمة :**ما الذي نجح؟ وما الذي فشل؟ ولماذا؟
- **تحديث خطة إدارة الأزمات** بناءً على الدروس المستفادة.
- إصلاح السمعة على المدى الطويل من خلال حملات اتصال استراتيجية.

لماذا إدارة الأزمات مهمة؟

1. **حماية السمعة والعلامة التجارية :**السمعة تستغرق سنوات لبنائها وثوانٍ لتدميرها. الإدارة الفعالة تحافظ على ثقة العملاء والمستثمرين.
2. **تقليل الخسائر المالية :**الأزمات يمكن أن تؤدي إلى خسائر مالية فادحة (توقف الإنتاج، غرامات، تعويضات). التخطيط يخفف هذه الخسائر.
3. **ضمان استمرارية الأعمال :**تساعد الخطة على استئناف العمليات الحيوية بأسرع وقت ممكن.
4. **حماية الموظفين والعملاء :**أولوية أي خطة لأزمة هي حماية صحة وسلامة الأفراد.
5. **الوفاء بالمسؤولية القانونية والأخلاقية :**الاستجابة المنظمة تقلل من المخاطر القانونية وتظهر أن المؤسسة مسؤولة.

العلاقة بين **الأمن المؤسسي وإدارة الأزمات**

العلاقة بين **الأمن المؤسسي وإدارة الأزمات** علاقة تكاملية ووثيقة جداً. لا يمكن لأحدهما أن يعمل بشكل فعال دون الآخر في بيئة المؤسسات الحديثة.

دعنا نشرح كلاً منهما ثم نستعرض طبيعة هذا التكامل.

أولاً: الأمن المؤسسي(Corporate Security)

المفهوم :هو الوظيفة المسؤولة عن حماية أصول المؤسسة المادية والمعنوية من المخاطر الداخلية والخارجية.

مجالات تركيزه:

- **الأمن المادي :**حراسة المنشآت، أنظمة التحكم في الدخول، كاميرات المراقبة.
- **أمن المعلومات :**حماية البيانات والأنظمة من الاختراق والتجسس.
- **السلامة والصحة المهنية :**منع الحوادث والإصابات في مكان العمل.
- **الأمن الفني :**تأمين البنية التحتية التكنولوجية.
- **الاستخبارات الأمنية :**جمع وتحليل المعلومات عن التهديدات المحتملة.

دوره: وقائي في الأساس .فهو "خط الدفاع الأول."

ثانياً: إدارة الأزمات(Crisis Management)

المفهوم :هو عملية التخطيط والاستعداد والاستجابة والتعافي من حدث مفاجئ وخطير يهدد استقرار المؤسسة أو سمعتها.

مجالات تركيزه:

- التخطيط للطوارئ.
- تشكيل فرق إدارة الأزمات.
- استراتيجيات الاتصال أثناء الأزمات.
- استمرارية الأعمال.
- إدارة السمعة.

دوره: تعامل مع الحدث بعد وقوعه (رد فعل منظم) .فهو "خط الدفاع الأخير" و"فريق الإسعاف."

طبيعة العلاقة التكاملية: كيف يعملان معاً؟

يمكن فهم العلاقة من خلال المراحل الزمنية للأزمة:

.1مرحلة **ما قبل الأزمة (الوقاية والاستعداد)**

- **دور الأمن المؤسسي :**هو العين الساهرة للمؤسسة. يقوم بـ:
  - **تحديد التهديدات:**من خلال تقييمات المخاطر (مثل: نقاط الضعف في المنشأة، ثغرات أمن المعلومات، تهديدات ضد الموظفين.(
  - **منع وقوع الأزمات :**بتنفيذ إجراءات أمنية استباقية (أنظمة إنذار، جدران حماية، تدريب الموظفين على السلامة) .**هنا، الأمن المؤسسي يمنع 90٪ من الأزمات المحتملة.**
  - **تغذية إدارة الأزمات بالمعلومات :**يزود فريق إدارة الأزمات ببيانات دقيقة عن المخاطر المحتملة لمساعدتهم في وضع خطط واقعية.
- **دور إدارة الأزمات :**يأخذ المعلومات من الأمن المؤسسي ويطور:
  - **خطط الاستجابة :**بناءً على سيناريوهات التهديدات التي حددها الأمن.
  - **برامج التدريب والمحاكاة :**لتدريب الجميع (بما فيهم فريق الأمن) على كيفية التصرف عند وقوع الأزمة.

.2مرحلة **أثناء الأزمة (الاستجابة والاحتواء)**

- **دور الأمن المؤسسي :**يتحول إلى "ذراع التنفيذ" لفريق إدارة الأزمات. يقوم بـ:
  - **تأمين موقع الأزمة :**عزل المنطقة، إخلاء المبنى، منع الوصول غير المصرح به.
  - **حماية الأدلة :**في حالة الأزمات الجنائية (مثل اختراق أو سرقة).
  - **ضمان السلامة الجسدية :**للعمال والزبائن.
  - **تقديم المعلومات الحيوية :**لفريق إدارة الأزمات عن تطور الموقف على الأرض.
- **دور إدارة الأزمات :**يتحول إلى "غرفة العمليات المركزية". يقوم بـ:
  - **تنسيق الجهود :**بين الأمن والإدارة والموارد البشرية والعلاقات العامة.
  - **اتخاذ القرارات الاستراتيجية :**بناءً على المعلومات الواردة من فريق الأمن.
  - **إدارة الاتصالات :**توجيه الرسائل الرسمية للجمهور الداخلي والخارجي.

.3مرحلة **ما بعد الأزمة (التعافي والتعلم)**

- **دور الأمن المؤسسي :**يقوم بـ:

- **التحقيق في جذور الأزمة :**ما الذي حدث بالضبط؟ وكيف حدث؟ ومن المسؤول؟
- **مراجعة الإجراءات الأمنية :**وتقويتها بناءً على الدروس المستفادة.
- **إعداد تقرير فني** عن الثغرات التي تم استغلالها.

- **دور إدارة الأزمات :**يقوم بـ:

- **تحليل أداء الخطة :**هل نجحت؟ أين كانت نقاط الضعف؟
- **تحديث خطة إدارة الأزمات** بناءً على التقرير المقدم من الأمن المؤسسي.
- **إدارة السمعة** على المدى الطويل.

التشبيه التوضيحي

تخيل المؤسسة كـ **سفينة:**

- **الأمن المؤسسي** هو :**الطاقم الفني ومراقبي الطقس** .مهمتهم فحص السفينة باستمرار، اكتشاف الأعطال، توقع العواصف، وإصلاح الثغرات قبل أن تتسبب في كارثة.
- **إدارة الأزمات** هي :**ربان السفينة وطاقم القيادة في غرفة** العمليات **عندما تضرب عاصفة مفاجئة (الأزمة)، مهمتهم هي توجيه السفينة، إعطاء الأوامر للطاقم، وإدارة عملية الإنقاذ للحفاظ على السفينة ومن عليها.**

الطاقم الفني (الأمن) لا يستطيع إنقاذ السفينة دون توجيه من القبطان (إدارة الأزمات)، والقبطان لا يستطيع فعل أي شيء دون معلومات وجهود الطاقم الفني.

الخلاصة

- **الأمن المؤسسي** هو **العمود الفقري الوقائي** لإدارة الأزمات.

- **إدارة الأزمات** هي **الإطار الاستراتيجي** الذي يعمل ضمنه الأمن المؤسسي عند وقوع الكارثة.

المؤسسة الناجحة هي التي تدمج بينهما في هيكل واحد متماسك، وتضمن تدفق المعلومات بينهما بسلاسة، وتفهم أن الاستثمار في الأمن المؤسسي هو جزء لا يتجزأ من الاستعداد الفعال لإدارة الأزمات.

العلاقات العامة وإدارة الازمات

أصبحت العلاقات العامة من أهم الأسس التي تعتمد عليها المؤسسات لضمان استمرارية عملها بنجاح، خاصة في ظل التغيرات السريعة في بيئة الأعمال والأزمات التي قد تواجهها، تمتد أهمية العلاقات العامة إلى دورها في إدارة الأزمات من خلال سلسلة متكاملة من الخطوات والمراحل التي تشمل الاستعداد للأزمات، الكشف المبكر عن المؤشرات المحتملة، الاستجابة الفورية، والتعافي بعد الأزمة. يتضمن هذا الدور استخدام استراتيجيات تواصل مدروسة تهدف إلى توجيه رسائل واضحة للجمهور المستهدف، سواء كان ذلك الجمهور عملاء، موظفين، أو وسائل الإعلام. وتعمل هذه الاستراتيجيات على الحد من تأثير الأزمة وطمأنة الجمهور عبر توفير معلومات دقيقة وشفافة عن الأوضاع والإجراءات التي تتخذها المؤسسة.

ويظهر دور العلاقات العامة بقوة في مراحل إدارة الأزمات، والتي تشمل الاستعداد المبكر وتقييم المخاطر، وتطوير قنوات التواصل السريعة لضمان وصول المعلومات إلى جميع الأطراف المعنية، واستراتيجيات التفاعل المباشر مع الجمهور المتأثر. وتشمل أيضًا استخدام وسائل الإعلام المختلفة كوسيلة فعّالة لنقل الرسائل واحتواء الأضرار

أهمية العلاقات العامة في إدارة الأزمات

تلعب العلاقات العامة دورًا محوريًا في حماية المؤسسات أثناء الأزمات، حيث تمثل خط الدفاع الأول للتصدي للتداعيات السلبية التي قد تنجم عن هذه الأزمات. وفيما يلي توضيح مفصّل لأهمية العلاقات العامة في إدارة الأزمات:

1. **حماية سمعة المؤسسة:**

أثناء الأزمات، يمكن أن تتعرض سمعة المؤسسة لضغوط شديدة نتيجة تداول معلومات سلبية أو شائعات قد تؤثر على ثقة الجمهور. هنا، يأتي دور العلاقات العامة في ضمان تقديم المعلومات الصحيحة في الوقت المناسب. يُعتمد في ذلك على توجيه رسائل إعلامية صادقة وواضحة إلى وسائل الإعلام والجمهور، مما يساعد في الحد من انتشار الأخبار الخاطئة والشائعات. تعكف فرق العلاقات العامة على إعداد البيانات الرسمية وإجراء مقابلات صحفية لشرح ما يجري وتوضيح موقف المؤسسة، وهو أمر مهم لتفادي تدهور السمعة وحماية صورة المؤسسة العامة.

2. التواصل الفعّال والمستمر:

يعد التواصل المستمر والشفاف مع الجمهور والعاملين ووسائل الإعلام أمرًا جوهريًا لإدارة الأزمة بفعالية. يُساعد هذا التواصل في طمأنة الجمهور وتقليل المخاوف. من خلال رسائل إعلامية مدروسة وقنوات اتصال مفتوحة، تعمل فرق العلاقات العامة على نقل التطورات بانتظام واحتواء الوضع؛ وذلك بإبقاء الجمهور على اطلاع بكل ما يحدث، مما يعزز من قدرة المؤسسة على إدارة الأزمة بفعالية.

يتم تنظيم المؤتمرات الصحفية، ونشر التحديثات عبر وسائل التواصل الاجتماعي، وتوفير خطوط هاتفية للاستفسارات، وذلك لضمان وصول الرسائل بطريقة شفافة وسريعة، مما يساهم في السيطرة على الموقف قبل تفاقمه.

3. إعادة بناء الثقة بعد الأزمة:

يعد الالتزام بالشفافية والمسؤولية خلال وبعد الأزمة من أهم خطوات العلاقات العامة لاستعادة الثقة. فبمجرد انتهاء الأزمة، تبدأ فرق العلاقات العامة في العمل على تحسين صورة المؤسسة وإعادة بناء ثقة الجمهور بها. يتم ذلك عبر تقديم تفسيرات وإجابات واضحة عن أسباب الأزمة، واتخاذ التدابير التي تمنع تكرارها.

على سبيل المثال، إذا كانت الأزمة ناتجة عن خطأ داخلي، تُظهر العلاقات العامة اعتراف المؤسسة بهذا الخطأ وتتخذ خطوات عملية لإصلاحه، مع تقديم وعود بأن المؤسسة ستتخذ كافة الإجراءات اللازمة لتلافيه في

المستقبل. تساعد هذه الاستراتيجية على إظهار مسؤولية المؤسسة وجديتها في تصحيح الأوضاع، وهو ما يعزز ثقة الجمهور ويعيد بناء سمعتها تدريجيًا.

4. تقديم خطط دعم طويلة الأجل:

تتطلب بعض الأزمات التي تخلف آثارًا طويلة الأمد خطط دعم مستدامة لتحسين صورة المؤسسة. هنا تظهر أهمية العلاقات العامة من خلال إطلاق مبادرات مجتمعية، أو المساهمة في برامج توعية، أو تقديم دعم مالي ومساعدات تعكس التزام المؤسسة تجاه الجمهور والمجتمع المتضرر.

باختصار، تعد العلاقات العامة ركيزة أساسية لإدارة الأزمات بفعالية، فهي توفر استراتيجيات تواصل شفافة وتعمل على حماية السمعة وبناء جسور الثقة مع الجمهور. هذه الأدوات تسمح للمؤسسات بعبور الأزمات بأقل الخسائر وبتعزيز مكانتها في المستقبل.

استراتيجيات العلاقات العامة في التعامل مع الأزمات

تلعب العلاقات العامة دورًا محوريًا في إدارة الأزمات عبر تطبيق مجموعة من الاستراتيجيات التي تساعد على احتواء الموقف وتوجيه الرأي العام بصورة إيجابية. فيما يلي توسع في أبرز هذه الاستراتيجيات التي تتبعها فرق العلاقات العامة للتعامل مع الأزمات:

1. الشفافية

الشفافية هي من الأساسيات في إدارة الأزمات؛ حيث تحرص فرق العلاقات العامة على تقديم الحقائق بوضوح وصدق دون إخفاء للمعلومات التي تهم الجمهور. من خلال الشفافية، يمكن للمؤسسة تعزيز ثقة الجمهور بها والحد من انتشار الشائعات. تلجأ فرق العلاقات العامة إلى إصدار بيانات واضحة تشرح طبيعة الأزمة، والآثار المحتملة لها، وكيفية تعامل المؤسسة معها. يساهم هذا في منع الأفراد من التلاعب بالمعلومات ويساعد الجمهور على فهم الموقف وتجنب بناء توقعات خاطئة.

2. سرعة الاستجابة

تعتبر سرعة الاستجابة عنصرًا بالغ الأهمية في إدارة الأزمات. فالتأخير في الرد على الأزمات قد يفتح المجال لتأويلات سلبية وشائعات تؤدي إلى تزايد المخاوف والقلق بين الجمهور. لذا، تحرص فرق العلاقات العامة على إصدار بيان رسمي أو تقديم توضيح سريع يشرح ما يحدث، حتى وإن كانت المعلومات الأولية محدودة. يُعد التواصل الفوري مع الجمهور خطوة فعالة لطمأنتهم ومنع تصاعد الأزمة.

3. التعاطف

يُعتبر إظهار التعاطف مع المتأثرين من الأزمة استراتيجية فعالة في كسب تأييد الجمهور وتعزيز مشاعرهم الإيجابية تجاه المؤسسة. يظهر التعاطف من خلال تقديم اعتذار صادق أو توضيح يظهر دعم المؤسسة للمتضررين أو تعاطفها مع الجمهور. هذه الخطوة تساعد على تقليل مشاعر الغضب والاستياء وتظهر الجانب الإنساني للمؤسسة. يمكن للتعاطف أن يتم عبر وسائل التواصل الاجتماعي أو بيانات إعلامية عامة تركز على دعم المتأثرين وطرح حلول للمساعدة.

4.تقديم الحلول

تعد استراتيجية تقديم الحلول إحدى الطرق العملية التي تتبعها العلاقات العامة لإدارة الأزمات. فبدلاً من التركيز فقط على الاعتذار أو التوضيح، تُظهر فرق العلاقات العامة الخطوات الفعلية التي ستتخذها المؤسسة لمعالجة الأزمة وتفادي تكرارها. هذا يعزز ثقة الجمهور بأن المؤسسة تتحمل المسؤولية وتعمل بجدية لحل المشكلة. قد تتضمن الحلول إجراء تحقيقات داخلية، وتطبيق إجراءات وقائية، أو اتخاذ تدابير لمعالجة الآثار الناجمة عن الأزمة. يساعد تقديم الحلول الفعالة على إظهار التزام المؤسسة بالتحسين واستعادة سمعتها بعد انتهاء الأزمة.

5. التواصل المستمر وتحديثات الوضع

التواصل المستمر خلال الأزمة يعد من الأمور الضرورية؛ فالجمهور يرغب في معرفة تطورات الأحداث وتحديثات الوضع بشكل منتظم. تعمل فرق العلاقات العامة على توفير معلومات مستمرة تُبقي الجمهور على اطلاع بما يحدث. ويتم ذلك عبر بيانات متكررة، نشرات إخبارية، وتحديثات على منصات التواصل الاجتماعي والموقع الإلكتروني الرسمي للمؤسسة. يساهم هذا التواصل في تعزيز ثقة الجمهور بأن المؤسسة تدير الأزمة بجدية ومسؤولية، ويساهم في تهدئة الوضع العام.

باختصار، تضمن استراتيجيات العلاقات العامة التعامل مع الأزمات بطريقة مهنية وفعالة، حيث يتم التركيز على الشفافية، سرعة الاستجابة، والتعاطف، بالإضافة إلى تقديم الحلول وتحديثات مستمرة للوضع، مما يساعد على تعزيز ثقة الجمهور وإدارة الأزمة بأقل قدر ممكن من الأضرار.

الأخطاء الشائعة في إدارة الأزمات وكيفية تجنبها

تُعتبر إدارة الأزمات عملية حساسة تتطلب اتخاذ قرارات سريعة وفعّالة، ولكن العديد من المؤسسات قد تقع في أخطاء تزيد من حدة الأزمة. فيما يلي بعض الأخطاء الشائعة التي تواجهها المؤسسات، مع توضيح كيفية تجنبها لضمان استجابة ناجحة للأزمات.

1. التأخر في الاستجابة

المشكلة : عند حدوث أزمة، فإن التأخر في إصدار بيان رسمي يزيد من احتمالية انتشار الشائعات والمعلومات المغلوطة حول الأزمة. هذا التأخر قد يجعل الجمهور يعتقد أن المؤسسة تتجاهل الأزمة أو غير قادرة على معالجتها، مما يؤدي إلى زيادة القلق وفقدان الثقة.

كيفية تجنبه:

يمكن للمؤسسات تجنب هذا الخطأ من خلال وضع خطط استباقية للأزمات تتضمن إجراءات واضحة للاستجابة السريعة. يُفضل أن تكون هناك فرق مخصصة لإدارة الأزمات تتمتع بالخبرة في التواصل السريع

وإعداد البيانات الأولية فور حدوث الأزمة. بالإضافة إلى ذلك، يمكن إصدار بيان مبدئي حتى مع توفر معلومات محدودة، يوضح أن المؤسسة على دراية بالأزمة وتعمل على معالجتها، مما يساهم في تهدئة الجمهور.

2. إنكار الأزمة

المشكلة:

يعتبر إنكار الأزمة من أخطر الأخطاء التي يمكن أن تقع فيها المؤسسات، حيث يؤدي إلى شعور الجمهور بعدم الثقة في المؤسسة. إنكار أو التقليل من حجم الأزمة يترك انطباعًا بأن المؤسسة غير صادقة، وقد يُعتبر هذا الإنكار إهانة للمجتمع المتأثر بالأزمة، مما يؤدي إلى تضرر صورة المؤسسة على المدى البعيد.

كيفية تجنبه:

يجب أن تتجنب المؤسسة إنكار الأزمة بأي شكل، وأن تعترف بالأزمة وتتعامل معها بشكل شفاف. حتى إن لم تكن المؤسسة مستعدة بعد لمعالجة الأزمة، يجب عليها أن تبين موقفها وتعلن عن خططها لمعالجة الوضع. الاعتراف بالأزمة يظهر احترام المؤسسة لجمهورها ويعزز من مصداقيتها، مما يساعد على استعادة الثقة حتى في أوقات الأزمات.

3. نقص الشفافية

المشكلة: محاولة إخفاء معلومات مهمة حول الأزمة قد يدفع الجمهور لاعتبار المؤسسة غير صادقة أو تحاول التلاعب بالمعلومات. نقص الشفافية يُعزز من فرص انتشار الشائعات ويدفع الجمهور إلى البحث عن مصادر بديلة قد تكون غير دقيقة.

كيفية تجنبه: تجنب هذا الخطأ يتمثل في اعتماد الشفافية كأسلوب رئيسي في إدارة الأزمة. يجب على المؤسسة توفير معلومات دقيقة وحديثة حول تطورات الأزمة بشكل دوري، حتى لو كانت المعلومات لا تزال غير مكتملة. يمكن للمؤسسة التواصل مع الجمهور عبر وسائل التواصل الاجتماعي، والنشرات الإخبارية، وبيانات صحفية

توضح بشكل متكرر موقف المؤسسة والإجراءات المتخذة. هذا يساعد الجمهور على متابعة الموقف من مصدر موثوق ويمنع التضليل الإعلامي.

4. عدم الاستعداد المسبق للأزمات

المشكلة: قد تتعامل بعض المؤسسات مع الأزمات بشكل ارتجالي بسبب عدم وجود خطط أو تجهيزات مسبقة للتعامل مع حالات الطوارئ، مما يؤدي إلى قرارات عشوائية وتواصل ضعيف.

كيفية تجنبه: للتجنب، على المؤسسات تطوير خطط طوارئ تتضمن جميع السيناريوهات المحتملة للأزمات وتدريب الفرق بشكل منتظم. تساهم الخطط المسبقة في الاستجابة السريعة والفعالة عند وقوع الأزمة، حيث يكون لدى الفرق أدوات وإجراءات جاهزة لتنفيذها فورًا.

5. تقديم وعود غير واقعية

المشكلة: في بعض الأحيان، تحت ضغط الأزمة، قد تُقدّم المؤسسات وعودًا غير واقعية حول حل الأزمة بسرعة أو معالجة جميع الأضرار، مما قد يكون من الصعب تحقيقه. وعود غير قابلة للتنفيذ تؤدي إلى إحباط الجمهور وتعزز شعورهم بأن المؤسسة تفتقد للمصداقية.

كيفية تجنبه: يجب على المؤسسات تقديم وعود تتماشى مع قدراتها ومواردها. التواصل مع الجمهور يجب أن يكون دقيقًا وواقعيًا حول الحلول المتاحة ومدى الوقت المتوقع لتجاوز الأزمة. الشفافية بشأن التحديات والإجراءات المحددة التي ستتخذها المؤسسة يضمن الحفاظ على الثقة ويجنبها الاتهام بالمبالغة أو عدم الجدية.

6. تجاهل متابعة وتقييم ما بعد الأزمة

المشكلة: قد تعتبر بعض المؤسسات أن الأزمة قد انتهت بمجرد انحسار آثارها المباشرة، وتنسى أهمية متابعة وتقييم نتائج الاستجابة للأزمة، مما يجعل المؤسسة عرضة لتكرار الأخطاء في المستقبل.

كيفية تجنبه: التقييم هو جزء أساسي من إدارة الأزمات ويجب ألا يُهمل. بعد انتهاء الأزمة، من الضروري عقد اجتماع لتقييم الأداء وتحليل الأخطاء وتوثيق الدروس المستفادة. يمكن أيضًا جمع آراء الجمهور وموظفي المؤسسة حول إدارة الأزمة لتحسين الأداء المستقبلي وتطوير خطط أفضل.

باتباع هذه الخطوات والتجنب للأخطاء الشائعة في إدارة الأزمات، تستطيع المؤسسات تحسين تعاملها مع الأزمات بشكل كبير، مما يعزز من ثقة الجمهور ويحافظ على سمعة المؤسسة وفعاليتها في المستقبل.