Region Örebro län

Rapport
Datum: 2022-04-27
Författare: Anneli Björkholm

# Årsrapport Informationssäkerhet 2021

Version: 1

# Årsrapport Informationssäkerhet 2021

Enheten för juridik och informationssäkerhet
Informationssäkerhetssamordnare Anneli Björkholm,
Enhetschef för juridik och informtionssäkerhet Sofia Öhrman

2022-04-27
Dnr: 22RS4118

# Innehåll

# 1. Sammanfattning

Informationssäkerhet handlar om att skydda information på ett säkert sätt. Det gäller all slags information oavsett var den finns lagrad, exempelvis på papper, digitalt eller muntligt. Information är en av Region Örebro läns (nedan regionen) viktigaste tillgångar. Det är även en förutsättning för en säker och effektiv verksamhet samt en förutsättning för en säker och bra digitalisering.

Regionen ska bedriva ett systematiskt informationssäkerhetsarbete. Det systematiska arbetet med informationssäkerhet och utveckling av regionens säkerhetskultur blir allt viktigare då alltmer information finns tillgänglig digitalt och hanteras/behandlas av olika leverantörer. Detta medför också risker, genom it-attacker kan information göras otillgänglig eller gå förlorad. Riskerna måste därför fångas upp och hanteras, rätt säkerhetskrav måste ställas på leverantörer i rätt tid.

It-attackerna har även under 2021 fortsatt att öka. Regionen har inte drabbats men det har andra organisationer i Sverige och världen gjort. Många intrångsförsök via e-posten har skett i regionen och omfattningen har ökat under pandemin. En god säkerhetskultur och ett systematiskt informationssäkerhetsarbete är viktigt.

Informationsklassningar och riskanalyser behöver ske i verksamheter som hanterar information. Det är grunden i det systematiska informationssäkerhetsarbetet och dataskyddsarbetet som ska finnas i alla regioner och kommuner. Således är det här ett ständigt återkommande arbete för regionen liksom för alla andra organisationer som hanterar information.

De uppföljningar som skett av informationssäkerhetsarbetet och säkerhetskultur i regionen visar på ett behov av att öka kunskapen kring informationssäkerhet i stort, i synnerhet kunskapen om ansvar och roller, vem som är informationsägare och vad innebär det att vara informationsägare etc. Områdena uppföljning och utvärdering, upphandling och utveckling av säkerhetskultur är viktiga områden som behöver utvecklas.

Uppföljningarna visar vidare att informationsklassningar och riskanalyser till viss del genomförs i organisationen men med varierande kvalité. För att förbättra arbetet i regionen behöver kunskapen stärkas. Vidare behöver verktygen för informationsklassning och riskanalys förenklas.

# 2. Bakgrund

Information är en av regionens viktigaste tillgångar. Det är även en förutsättning för en säker och effektiv verksamhet samt en förutsättning för digitaliseringen. Informationssäkerhet handlar om att skydda information på ett säkert sätt. Det gäller all slags information oavsett var den finns lagrad, exempelvis på papper, digitalt eller muntligt.

Regionen ska bedriva ett systematiskt informationssäkerhetsarbete med utgångspunkt enligt den svenska och internationella standarden för informationssäkerhet SS-ISO/IEC 27001:2017 (Ledningssystem för informationssäkerhet). I det systematiska informationssäkerhetsarbetet ska hot, sårbarheter och risker identifieras samt säkerhetsåtgärder införas som reducerar dessa till en för regionen acceptabel nivå med hänsyn till konfidentialitet, riktighet och tillgänglighet. Medborgarna ska kunna lita på den information regionen hanterar och att den skyddas på ett bra vis.

Ett systematiskt informationssäkerhetsarbete innebär att strukturerat planera, avsätta resurser, fatta medvetna beslut för att skydda rätt information på rätt sätt. Det systematiska informationssäkerhetsarbete ska bedrivas för att stärka förmågan att undvika negativa händelser som påverkar regionens verksamheter. Inträffar en negativ händelse ska denna kunna hanteras på en godtagbar nivå med bibehållet förtroende från regionens intressenter.

Bedrivs inte informationssäkerhetsarbetet enligt de lagkrav som ställs kan det innebära konsekvenser som att informationssäkerhetsarbetet inte kan bedrivas med den kvalitet som förväntas vilket kan resultera i att regionens informationstillgångar inte hanteras på ett korrekt sätt. Detta kan vidare leda till sanktionsavgifter.

Ledningens genomgång är en viktig del enligt standarden för informationssäkerhet (SS-ISO/IEC 270001:2017) och ett krav enligt Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter inom hälso- och sjukvården (HSLF-FS 2016:40). Syftet med genomgången är att tillsammans med ledningen gå igenom och se över det systematiska informationssäkerhetsarbetet och dess styrning. Årsrapporten för informationssäkerhet är en del av denna genomgång för att säkerställa informationssäkerhetsarbetet och styrningens fortsatta lämplighet, tillräcklighet och verkan.

Denna rapport är framtagen på enheten för juridik och informationssäkerhet. Informationssäkerhetssamordnaren har samlat in material genom enkätuppföljningar och förfrågningar/intervjuer med representanter från alla regionens förvaltningar. Utifrån detta har rapporten sammanställts av informationssäkerhetsamordnaren och

enhetschef för juridik och informationssäkerhet. Avsnitt 7.1.1 och 7.1.2 har skrivits av medarbetare på Regionservice IT.

## 2.1 Informationssäkerhetspolicy

Den svenska och internationella standarden för informationssäkerhet, SS-ISO/IEC 27001:2017 ska vara en utgångspunkt för informationssäkerhetsarbetet. Ett regelverk för informationssäkerhet som inkluderar en informationssäkerhetspolicy ska enligt standarden fastställas och godkännas av ledningen.

Enligt Socialstyrelsens föreskrifter HSLF-FS 2016:40 ska varje vårdgivares ledningssystem innehålla en informationssäkerhetspolicy. I informationssäkerhetspolicyn beskrivs regionens mål och principer för informationssäkerhet för alla verksamheter. Policyn ska bidra till ett professionellt förhållningssätt där informationssäkerhetsaspekter ska vägas in i beslut som rör hantering av information. Policyn omfattar all information oavsett i vilken forms den lagras eller hanteras. Nuvarande informationssäkerhetspolicy fastställdes 2015 och uppdaterats under 2020. Under 2022 kommer en ny uppdatering av den befintliga policyn ske i syfte att förtydliga och förbättra informationssäkerhetsarbetet.

# 3. Informationssäkerhetsarbetet i regionen

## 3.1 Bemanning och organisation

Informationssäkerhetsarbetet i regionen utgår från Enheten för juridik och informationssäkerhet. Där är även informationssäkerhetssamordnaren samt dataskyddsombudet placerade.

Informationssäkerhetssamordnaren arbetar strategiskt med informationssäkerhet. Detta genom att exempelvis säkerställa att styrande och stödjande dokument finns på plats, genomföra utbildningar och informationsinsatser, ge råd och stöd. Arbetet är även av operativ karaktär. Dataskyddsombudets roll är till stor del reglerad genom EU:s dataskyddsförordning, GDPR. Exempelvis ska dataskyddsombudet ge råd och stöd, erbjuda utbildningar men även genomföra tillsyn samt anmäla brister i verksamheterna till Integritetsskyddsmyndigheten, IMY. Enhetschefen för juridik och informationssäkerhet arbetar till övervägande del med informationssäkerhet- och dataskyddsfrågor tillsammans med informationssäkerhetssamordnaren och dataskyddsombudet.

Regionen har ett informationssäkerhetsråd med representanter från samtliga förvaltningar. Informationssäkerhetsrådets uppdrag är att stödja och utveckla regionens systematiska informationssäkerhetsarbete på en övergripande nivå. Rådet och rådets medlemmar utgör en kanal för informationssäkerhetsfrågor mellan Regionkansliet och övriga förvaltningar inom regionen. Rådet rapporterar till regionens ledningsgrupp. Informationssäkerhetsrådet har fyra planerade möten per år. Vid behov kan fler möten hållas. Rådet är vidare en remissinstans för ex. styrande dokument.

Rådet besår av följande medlemmar: Enhetschef för juridik och informationssäkerhet (ordförande), informationssäkerhetssamordnare, dataskyddsombud, chef säkerhets- och beredskapsenheten, representant för Staben för digitalisering, IT-säkerhetsansvarig, It- chef, representant från upphandling samt MT, förvaltningsövergripande chefläkare, beredskapsläkare samt en representant från övriga regionens förvaltningar.

## 3.2 Informationssäkerhetsarbetet under 2021

Regionens informationssäkerhetsarbete ska bedrivas systematiskt och riskbaserat. För att hitta rätt nivå av skydd för den information som regionen hanterar är det viktigt att utgå från värdet av informationen och de risker som finns. Det ska göras genom informationsklassning och riskanalys av regionens informationstillgångar.

All information ska ha en identifierad ägare. Informationsägare är den som äger och ansvarar för den information som skapas och används inom verksamheten. Ansvar som informationsägare följer det delegerade verksamhetsansvaret. I de fall där det finns ett flertal informationsägare likställs rollen objektägare med informationsägare enligt regionens förvaltningsmodell för it.

Informationssäkerhetsarbetet har även under 2021 påverkats av den rådande pandemin. Under 2021 har it-attackerna fortsatta att öka mot myndigheter och företag både i Sverige och i andra länder Bland annat så råkade företaget Coop ut för en it-attack som gjorde att kassasystemet inte fungerade under ca en vecka. It-attacken riktades mot en av Coops underleverantörer (en amerikansk underleverantör) men drabbade alla som hade denna leverantör i sin leverantörskedja. It- attacken som drabbade Kalix kommun resulterade i ett omfattande arbete och höga kostnader. Hela It- systemet slogs ut och exempelvis kunde inga löneutbetalningar ske, hälso- och sjukvårdsinformation var otillgänglig och en övervägande del av alla datorer fick installeras om. Händelsen pågick över en månad. Det blir tydligt hur viktigt det är att skydda verksamhetens informationstillgångar.

MSB har även under 2021 fortsatt att hålla möten med regioner och andra myndigheter varje vecka där aktuella hot och risker tas upp. Dessa möten gör att alla tillsammans kan agera snabbare vid händelser och framför allt förebygga att incidenter inträffar.

Det finns ett behov av att öka kunskapen kring informationssäkerhet i stort, i synnerhet kunskapen om ansvar, vem som är informationsägare och vad innebär det att vara informationsägare. Informationsklassningar och riskanalyser genomförs till viss del i organisationen med varierande kvalité. Det finns fortsatt ett stort behov av att öka kunskapen i verksamheterna om hur informationsklassningar och riskanalyser sker. Fler personer i verksamheterna behöver utbildas för att kunna genomföra både klassningar och riskanalyser av regionens informationstillgångar.

Under 2021 har enheten för juridik och informationssäkerhet erbjudit flera informationstillfällen och utbildningsinsatser för olika grupperingar i syfte att öka kunskapen. Vidare har styrande och stödjande dokument uppdaterats och tillkommit för att höja kunskapen. Det är dock av stor vikt att fortsätta öka medvetenheten och höja kunskapsnivån generellt. Digitaliseringen går fortsatt väldigt snabbt och här måste informationssäkerheten fångas in i ett tidigt skede.

## 3.3 Dataskydd

Dataskydd utgör en del av informationssäkerheten. Det är exempelvis genom klassningar och riskanalyser kravställning på dataskydd och säkerhetsåtgärder kan ske. Informationssäkerhet och dataskydd hänger således nära ihop.

Arbetet med att säkerställa att regionens personuppgifter hanteras utifrån GDPR är ett ständigt pågående arbete. För att säkerställa att riktlinjer och rutiner följs ska interna kontroller, utifrån en tillsynsplan, ske årligen av regionens dataskyddsombud. Även oplanerade granskningar kan komma att ske, utifrån händelser i omvärlden eller inom regionen.

Under 2020 fick all planerad tillsyn ställas in och planeras om pga. pandemin så blev fallet även under 2021.

### 3.3.1 Överföring av personuppgifter till tredjeland

I takt med digitaliseringen har även en stor del av dataskyddsarbetet under 2021 har handlat om överföring av personuppgifter till tredjeland (dvs. länder utan för EU/EES). Detta mot bakgrund av den s k Schrems II domen som meddelades i juni 2020 av EU domstolen. I domen underkände EU domstolen överföringsmekanismen Privacy Shield. Privacy Shield kunde tidigare användas som lagligt stöd för att

överföra uppgifter till USA. I och med att denna överföringsmekanism underkändes så har möjligheten att överföra personuppgifter till USA starkt begränsats vilket skapat stora utmaningar för regionen liksom andra personuppgiftsansvariga i Sverige och Europa.

Schrems II domen har sedan den kom 2020 gett upphov till ett mycket omfattande och komplicerat arbete med PUB-avtal där leverantörer och underleverantörer har kopplingar till tredjeland, främst USA.

European Data Protection Board, EDPB, har antagit den slutgiltiga versionen av ”Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter”. Denna version är slutbehandlat och gällande sedan 18 juni 2021. Regionen har under 2021 påbörjat ett samarbete med andra regioner för att få fram gemensamma dokument för hantering av överföringar av personuppgifter till tredjeländer. Slutlig version kommer att presenteras under 2022. Detta samarbete kommer att resultera i en vägledning som verksamheterna kan använda inför bedömning om lagligheten av överföringen samt beskrivning av de steg som ska tas inför avtalsskrivandet.

### 3.3.2 Microsoft Office 365 och Teams

Under våren 2021 beslutades att regionen skulle införa en hybrid integration med Microsoft 365. En hybrid lösning innebär att verksamheterna avgör vilken information som ska lagras lokalt och vad som ska lagras i molnet. Inför detta beslut gjordes en rättsutredning om Microsoft Office och Teams.

Teams införs stegvis i två faser under 2021/2022 där fas ett innebär tillgång till chatt och mötesbokningar samt möten i Teams. Fas två innebär tillgång till att skapa team för grupper eller projekt, samarbeta, dela filer och använda verktyg som Planner , Forms och OneNote.

Informationssäkerhetssamordnare och jurist har varit delaktiga i arbetet med informationsklassning och riskanalys för införande av Teams som har letts av extern konsult. Resultatet av informationsklassning och riskanalysen visar att Teams med tillhörande applikationer så som One Note, Forms och Planner kan användas efter en bedömning av informationsinnehållet. Bedöms informationen vara av känslig karaktär, innehålla känsliga personuppgifter eller sekretess ska inte Teams eller tillhörande applikationer användas då informationen behandlas av leverantör utanför EU/EES i det här fallet till USA.

Efter genomförd klassning och riskanalys har ett arbete med att ta fram riktlinje, utbildningsmaterial och information påbörjats men arbetet intensifierades under början av 2022.

## 3.4 Externa och interna samarbeten

### 3.4.1 Allmänt

I takt med digitaliseringen har samarbetet mellan regionerna stärks, främst inom Sjukvårdsregionen Mellansverige, exempelvis när det gäller tecknande av PUB-avtal med externa leverantörer. Utifrån Schrems II domen ställs höga krav på regionerna vid tecknande av PUB-avtal. I många fall är det en fördel för regionerna att ställa gemensamma krav på informationssäkerhet och dataskydd på leverantörerna.

### 3.4.2 Hälso-och sjukvårdens informationssäkerhetsnätverk, HoSiS

HoSiS är först och främst ett nätverk för de som arbetar med eller har ett ansvar för arbetet med informationssäkerhet inom regionernas hälso- och sjukvård i Sverige. Syftet med nätverket är att ge de personer som har ett uppdrag att samordna och stödja arbetet med hälso- och sjukvårdens informationssäkerhet i regionerna möjlighet att utbyta kunskap och information med varandra.

Målet är att genom att delta i nätverksträffar erbjuda medlemmar ett stöd för sitt arbete inom informationssäkerhetsområdet i den egna organisationen samt att tillhandahålla ett forum för utbyte och omvärldsbevakning. Ambitionsnivån med nätverket är att stödja och styra aktiviteter utifrån gemensamt framtagna fokusområden samt att informera om SKR:s och MSB:s kommande aktiviteter.

### 3.4.3 Sjukvårdsregion Mellansverige

Informationssäkerhetsgruppen är underställd Samverkansnämndens Ledningsgrupp. Informationssäkerhetsgruppen består av medlemmar från sjukvårdsregionens sju regioner. Gruppens huvuduppgift är att utveckla samarbetet inom informationssäkerhetsområdet inklusive dataskydd och cyberssäkerhet, öka kompetensen inom området och synliggöra det samarbete som sker.

I arbetsgruppen ingår regionernas informationssäkerhetssamordnare/chefer, dataskyddsombud, jurister samt resurser med it-säkerhetskompetens. Gruppen har träffats digitalt fyra gånger under 2021.

### 3.4.4 Informationssäkerhetsnätverk i Örebro län

I länet finns ett nätverket bestående av deltagare från Transportstyrelsen, Örebro kommun, SCB, Försvaret, Universitetet, Länsstyrelsen och Regionen. Deltagarna arbetar med informationssäkerhet och/eller it- säkerhet.

Nätverket har träffats fyra gånger under 2021. Fokus har varit informationssäkerhetsfrågor kopplat till de attacker som har ökat i vårt samhälle och hur myndigheterna arbetar med dessa.

### 3.4.5 Regionservice IT-Cirt

2020 startades IT-Cirt (IT security Incident response Team). Syftet är att teamet ska hålla sig välinformerad om aktuella hot och inträffade säkerhetsincidenter i omvärlden samt för att säkerställa att olika hotbildscenarier och säkerhetsincidenter kan hanteras och proaktivt verka för ökad säkerhet. It-cirt har en nära koppling till MSB:s CIRT grupp. Informationssäkerhetssamordnare deltar i it-cirt gruppens regelbundna avstämningar.

Förutom ovan nämnda samarbeten sker regelbunden avstämning mellan informationssäkerhetssamordnare och it-säkerhetsansvarig för informationsutbyte och diskussion avseende aktuella frågeställningar inom informationssäkerhetsområdet.

# 4. Granskningar och skyddsåtgärder

## 4.1 Informationsklassning och riskanalys

Risker som påverkar regionens informationssäkerhet ska identifieras, analyseras och behandlas samt återföljas av kontinuerlig uppföljning. Beslut om olika lösningar ska baseras på bedömd risk och informationstillgångarnas klassificeringsvärde. Informationsklassning är grunden för att genomföra en riskanalys då riskanalysen baseras på informationens värde.

Informationsägare är den som äger och ansvarar för den information som skapas och används inom verksamheten. Ansvar som informationsägare följer det delegerade verksamhetsansvaret.

Under 2021 har riskanalyser och informationsklassningar genomförts med varierande kvalité. Det finns ett stort behov av att öka kunskapen i verksamheterna. Fler personer i verksamheterna behöver utbildas för att kunna genomföra riskanalyser och informationsklassningar av regionens informationstillgångar. Informationsklassningar och riskanalyser är grunden i det systematiska informationssäkerhetsarbetet. Detta är således något som måste bli en naturlig del av all informationshantering, exempelvis vid upphandlingar, inköp, drift och förvaltning av it-stöd samt för hantering av information i verksamheternas processer.

Metoder, modeller och andra hjälpmedel i arbetet med riskanalyser och informationsklassningar behöver förenklas och struktureras ytterligare.

### 4.1.1 Rapportering från verksamheterna

Verksamheterna har rapporterat in följande gällande genomförda informationsklassningar med tillhörande riskanalyser.

**Vårdsystem**
17 stycken vårdsystem är informationsklassade, 0 återstår.

**Stödsystem**
55 stycken stödsystem är informationsklassade, 5 återstår och som ska planeras in under 2022. Ett övrigt system återstår för informationsklassning under 2022.

**Regionalutveckling**
Alla system är ännu inte informationsklassade men system som är kopplade till Serviceresor är klassade och åtgärder är vidtagna för att säkerställa korrekt hantering.

**Företagshälsovård samt tolk- och översättarservice**
I samband med införandet av GDPR informationsklassades förvaltningens verksamhetssystem. Någon ny översyn av informationsklassningen har inte genomförts under 2021. Det finns dock behov av att se över informationsklassningen av verksamheternas verksamhetssystem vilket inte kunnat prioriteras under året.

## 4.2 Granskningar

Ingen extern granskning eller tillsyn har utförts eller ägt rum under 2021

## 4.3 Skyddsåtgärder

### 4.3.1 Loggning och logguppföljning

Loggning och logguppföljning är en viktig del i regionens arbete med patientsäkerhet. Framför allt för att kunna visa att regionens hantering av personuppgifter sker på ett legalt och riktigt sätt men också för att kunna utreda misstankar om otillåten hantering av personuppgifter. Regionen är enligt lag skyldig att föra logg över elektronisk åtkomst inom vårdgivarens verksamhet och dokumentera regelbunden och systematisk loggkontroll.

Loggsystemet har alltid varit ett oförvaltat system. Under 2021 har ett arbete skett i syfte att få in loggsystemet i den ordinarie systemförvaltningen. Planen är att det under 2022 ska in i den ordinarie systemförvaltningen. .

### 4.3.2 Antal loggrapporter begärda av patienter

Under 2021 har 239 patienter begärt ut loggar över vilka anställda som tagit del av deras journaluppgifter. Därutöver har även verksamhetschefer begärt att få ut kompletterande loggar på medarbetare. Detta pga. att avvikelser upptäckts i de slumpvisa loggarna eller att verksamhetscheferna på annat sätt fått till sig uppgifter som gör att det uppkommit misstanke om obehörig åtkomst som behöver granskas vidare.

# 5. Uppföljningar

## 5.1 Uppföljning Infosäkkollen

Ett regeringsuppdrag har ställts till MSB (Myndigheten för samhällsskydd och beredskap) för att mäta framförallt förutsättningen för det systematiska informationssäkerhetsarbetet och i vilken utsträckning som det systematiska arbetet bedrivs. Resultatet av mätningen visar vilka åtgärder som behöver genomföras. En enkät skickades ut till regionerna för besvarande. Att delta i enkätundersökningen var frivilligt. Vidare kunde regionerna välja att behålla resultatet för sig själva eller att skicka in svaren. Regionen valde att besvara enkäten men inte att skicka in resultatet. Däremot har svaren analyserats internt och presenterats för bland annat informationssäkerhetrådet.

Frågeställningarna utgår från de kategoriserade arbetssätten för systematiskt informationssäkerhetsarbete och baseras därifrån på följande utvärderingsområden:

**Identifiera** och värdera informationstillgångar utifrån konfidentialitet, riktighet och tillgänglighet, **Bedöma** risker vid hanteringen av tillgångarna, **Införa** ändamålsenliga och proportionerliga säkerhetsåtgärder samt **Följa upp** och utvärdera.

Utvärderingsområden är sedan uppdelade på fyra nivåer:

- Nivå 1, Utforma (Grunderna för arbetet), Arbetssätt (mallar och riktlinjer) för Informationsklassning, Riskanalys, Incidenthantering, Kontinuitetshantering, Omvärldsbevakning, Utbildning, Upphandling mål och inriktning.

- Nivå 2, Tillämpning av grunderna Mäta lära, Utvärdera Genomförda informationsklassningar, Analyser av risker enligt beslutat arbetssätt, Beslut för tillsättning av resurser för säkerhetsåtgärder, Utvärdering av införda säkerhetsåtgärder, Kontinuitetsplanering, Arbetssätt vid Upphandling.

- Nivå 3, Mäta, Lära och Följa upp och förbättra, Om det systematiska informationssäkerhetsarbetet har ett kvalificerat innehåll och kan förväntas vara ändamålsenligt enligt ISO 27000.

- Nivå 4, Avancerat arbete med ständiga förbättringar enligt LIS.

### 5.1.1 Resultat

Regionen har de grundläggande delarna på plats; en informationssäkerhetspolicy, beskrivning av roller och ansvar, en riktlinje för informationsklassning, ett verktyg för informationsklassning och riskanalys samt rutiner för incidenthantering.
Mätningen för det systematiska arbetet visar att regionen brister i några aspekter.

Ett första steg för en förbättring är att uppnå alla delar i Nivå 1. Det innebär att regionen måste förbättra områdena uppföljning och utvärdering, upphandling och utveckling av säkerhetskultur. I detta arbete är bland annat ledningssystem för informationssäkerhet (LIS) och kravställning vid upphandling viktiga delar.


Digitaliseringstakten ökar och fler tjänster läggs ut på externa leverantörer. Det innebär också att alltmer information finns tillgänglig digitalt och behandlas/hanteras

av olika leverantörer. Detta medför också risker, genom it-attacker kan information göras otillgänglig eller gå förlorad. Det systematiska arbetet med informationssäkerhet och utveckling av vår säkerhetskultur blir allt viktigare.

Kraven på regionen är höga både tekniskt och juridiskt. Interna och externa krav förändras ständigt, vilket gör att informationssäkerhetsarbetet nära och i samverkan med verksamheterna är viktigare än någonsin. För att uppnå rätt nivå av informationssäkerhet är det centralt att arbetet med informationssäkerhet genomsyrar processerna i den löpande verksamheten. Det ska leda till att det blir en naturlig del i den ordinarie verksamheten och kulturen. Detta innebär att chefer och medarbetare förstår och accepterar sitt ansvar inom informationssäkerhet.

## 5.2 Uppföljning av informationssäkerhetsarbetet i regionen Intern styrning och kontroll (ISK)

Intern styrning och kontroll (ISK) är en process där regionstyrelsen, nämnderna och verksamhetsledningar har för att tillsammans upprätthålla en effektiv ledning och styrning av verksamheten. Processen ska säkerställa en ändamålsenlig och lagenlig verksamhet, det vill säga att verksamheten bedrivs i enlighet med de krav som ställs på verksamheten. För att säkerställa att kraven är uppfyllda finns i uppföljningen av ISK-processen beskrivningar av risken samt vad som förväntas av förvaltningarna när det gäller rapportering av informationssäkerhetsarbetet. När det gäller informationssäkerhetskraven ska dessa vara tillgodosedda utifrån kraven på konfidentialitet, riktighet, tillgänglighet samt spårbarhet.

För att säkerställa att kraven var uppfyllda under 2021 fanns i uppföljningen av ISK-processen beskrivningar av risken samt vad som förväntades av förvaltningarna när det gäller rapportering av informationssäkerhetsarbetet.

Risken att verksamheten inte efterlever tillämplig dataskyddslagstiftning (GDPR och Patientdatalagen). Samt NIS-direktivet och lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Regionövergripande åtgärder inför 2021:

- Säkerställa ett systematiskt och riskbaserat informationssäkerhetsarbete med användande av de resurser som i prioritering i förhållande till andra angelägna verksamheter, kan anslås.
- All berörd personal ska ha god kunskap om och medverka till att följa regelverk för informationssäkerhet.

- Att informationsklassa och riskbedöma vid inköp, upphandling och förändring som kan påverka informationssäkerheten.

Förvaltningarna har rapporterat för 2021. I rapporteringen framgår att vissa förvaltningar har avsatt resurser för sitt informationssäkerhetsarbete. För att öka kunskapen om roller och ansvar samt förståelsen för vad ett systematiskt informationssäkerhetsarbete är behövs informationsinsatser då ett systematiskt riskbaserat informationssäkerhetsarbete kräver kontinuerlig översyn och uppföljning för att motverka eventuellt nya uppkomna säkerhetsbrister.

## 5.3 Enkätuppföljning – i syfte att mäta kunskap och informationssäkerhetskultur i regionen

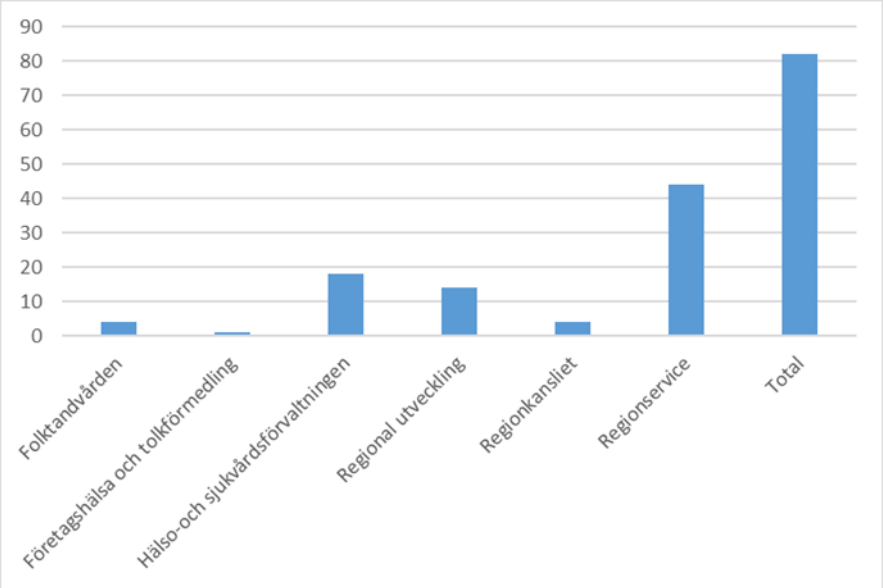
I slutet på 2021 och början av 2022 genomfördes en enkätundersökning i regionen. Enkäten riktade sig primärt till informationsägare i de olika förvaltningarna och skickades ut via medlemmarna i informationssäkerhetsrådet. Frågorna i enkäten handlade om grundläggande kunskaper om innehållet i exempelvis informationssäkerhetspolicy, riktlinjer och rutiner gällande informationssäkerhet. Syftet med enkätuppföljningen är att mäta kunskapsnivån och informationssäkerhetskulturen i regionen.

Regionen har de grundläggande delarna på plats, informationssäkerhetspolicy, beskrivning av roller och ansvar, riktlinje för informationsklassning, verktyg för informationsklassning och riskanalys och rutiner incidenthantering.

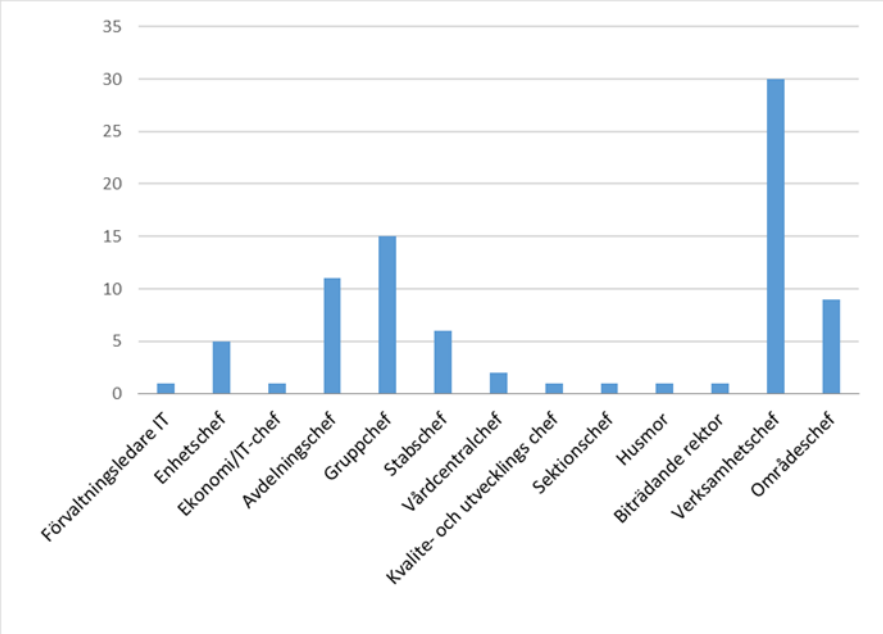
Enkätresultatet visar dock att mer information och kunskap behövs i de grundläggande delarna om ex. roller och ansvar. Verksamheterna efterlyser stöd i sitt systematiska informationssäkerhetsarbete när det gäller utförande av informationsklassningar, riskanalyser av den klassade informationsmängden samt vid tecknande av PUB-avtal.

Enligt enkätsvaren verkar en uppfattning vara att detta ansvar till stor del ligger på Regionsservice IT, MT samt Upphandlingsavdelningen.  Det är dock informationsägaren som bär det ansvaret likaså är informationsägaren ansvarig för att uppföljningar regelbundet sker.  Resultatet av enkäten är likvärdigt med resultatet av Infosäkkollen. I regionen behövs kunskap om informationssäkerhet och informationssäkerhetsarbetet stärkas, bland annat när det gäller innebörden av roller och ansvar.

Det varierande antalet i svar är beroende av hur varje förvaltning har valt att organisera informationssäkerhetsarbetet samt till vilka funktioner som frågorna har skickats för besvarande.



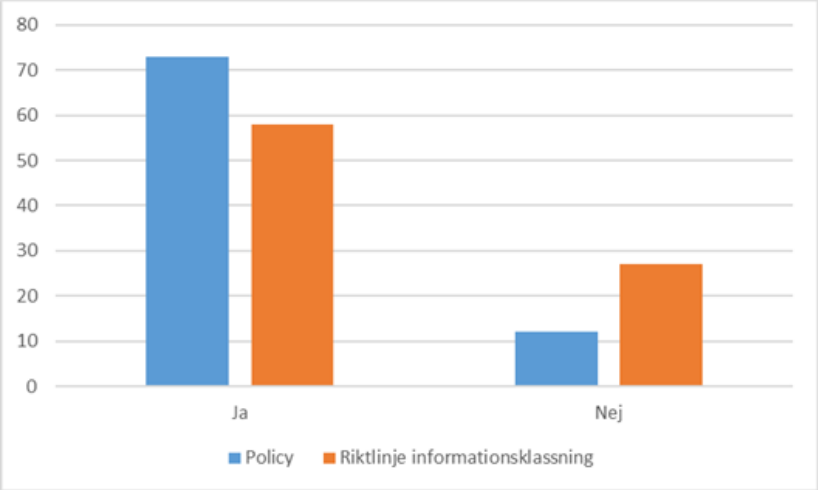

Roller i verksamheterna som har besvarat enkäten



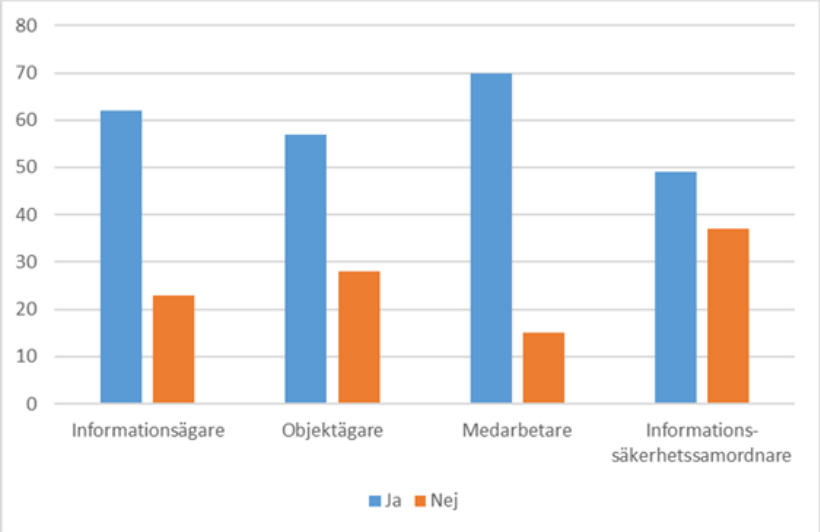
**Kännedom om roller och ansvar kopplat till informationssäkerhetsarbetet enligt informationssäkerhetspolicy samt riktlinje för informationsklassning**

Har du läst regionens policy för informationssäkerhet?

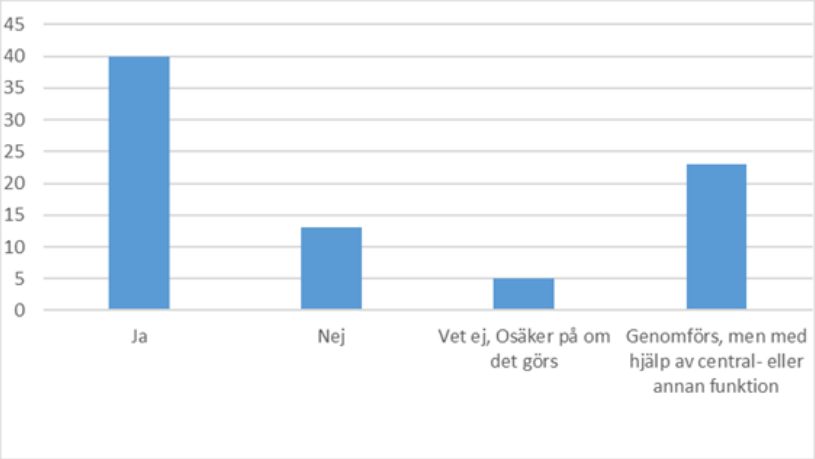
Har du läst regionens riktlinje för informationsklassning?



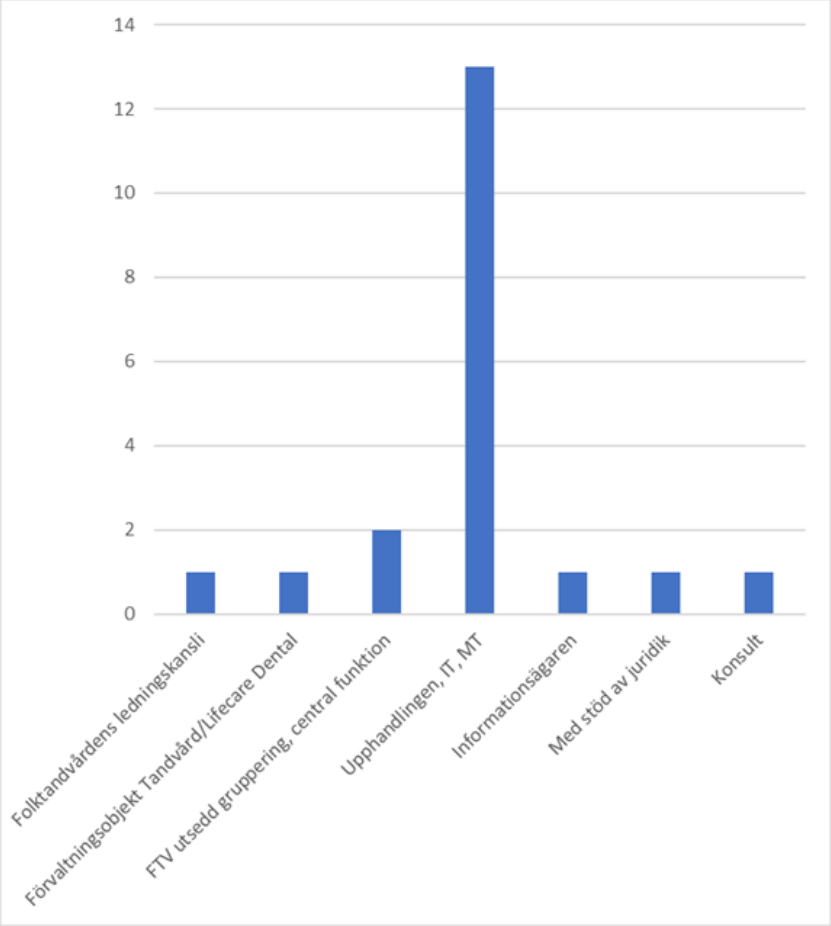

Känner du till de roller som finns i samband med informationssäkerhet och vad de innebär?



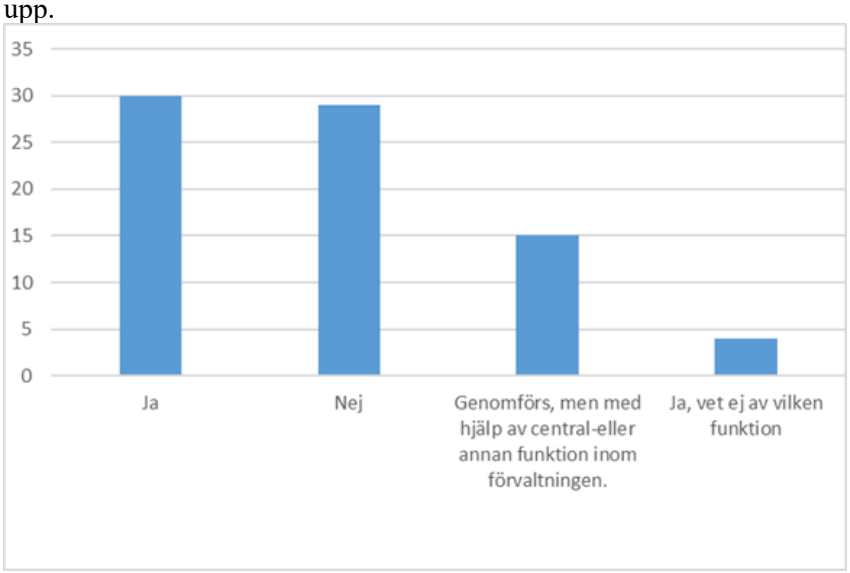
**Frågeställning informationsklassning och riskanalyser och uppföljning**
Genomförs informationsklassning och riskanalyser vid inköp av nya licenser, programvaror och avtal?



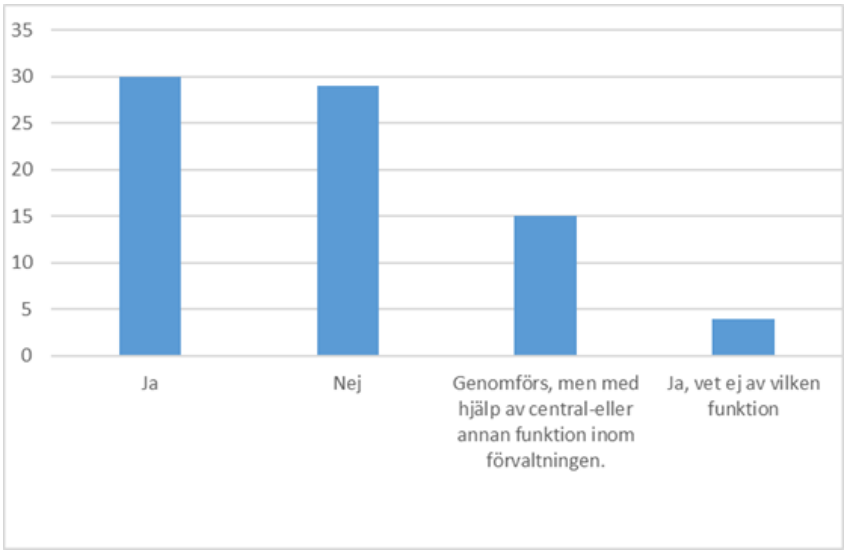

Annan funktion:



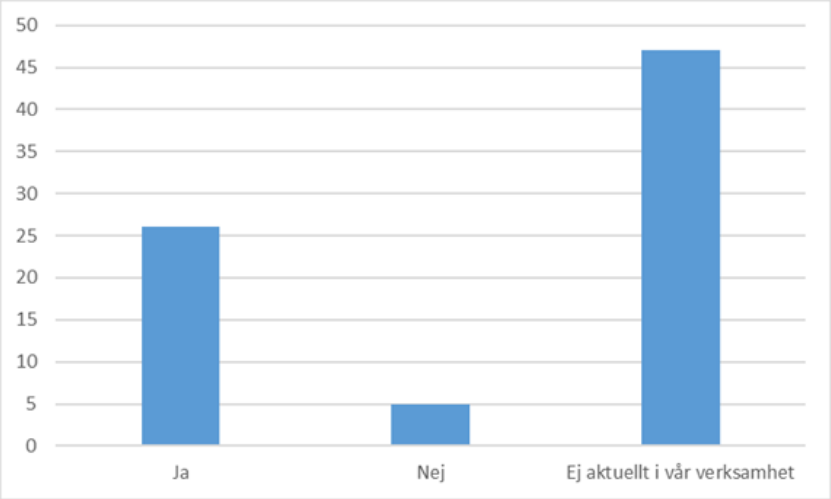
Risker och åtgärder kopplade till genomförd informationsklassning följs regelbundet upp.




Vid de tillfällen där licens/avtal tecknas med extern leverantör tecknas alltid ett PUB-avtal enligt de riktlinjer som finns för personuppgiftsbehandling av externa parter.

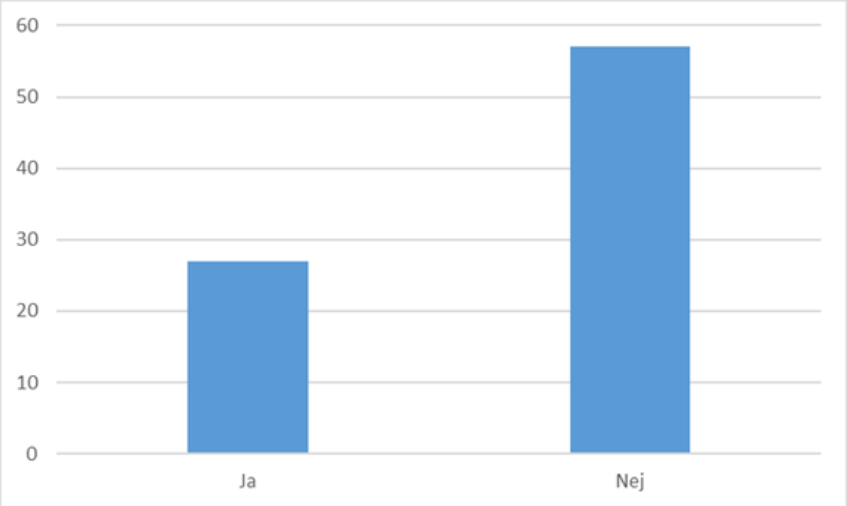



Enligt kraven från patientdatalagen (PDL) loggas all åtkomst till patientuppgifter där bl.a. tidpunkt, åtgärd och användarens identitet framgår. Slumpvisa loggkontroller sker för att upptäcka eventuell otillåten åtkomst. Följs upptäckten av eventuell otillåten åtkomst upp av dig som verksamhetschef?

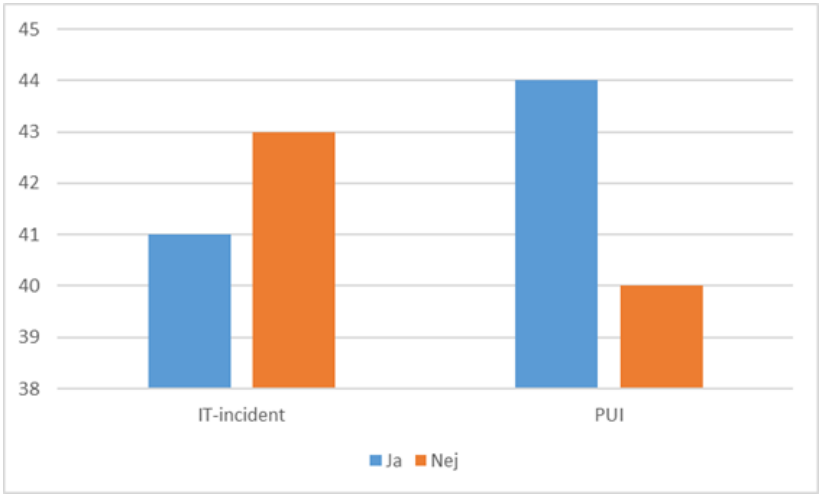



**Frågeställning Utbildning och Information**

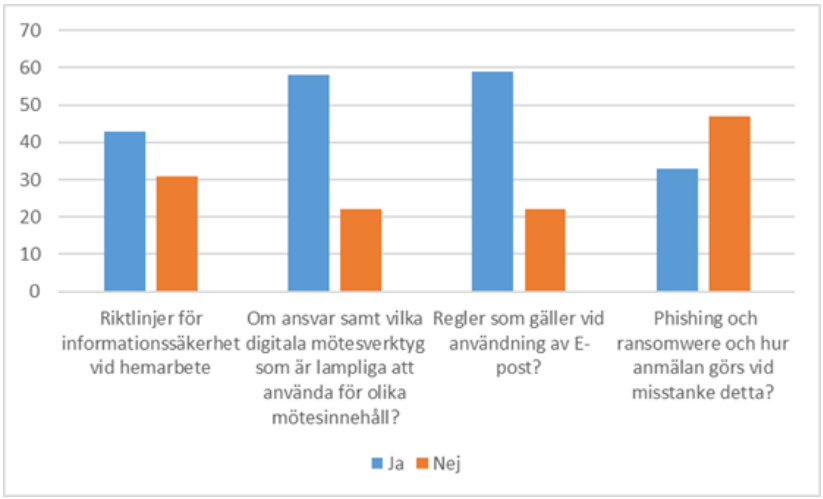
Har alla medarbetare genomfört e-learningsutbildningen i regionens utbildningsportal "PINGPONG" om informationssäkerhet och sekretess?



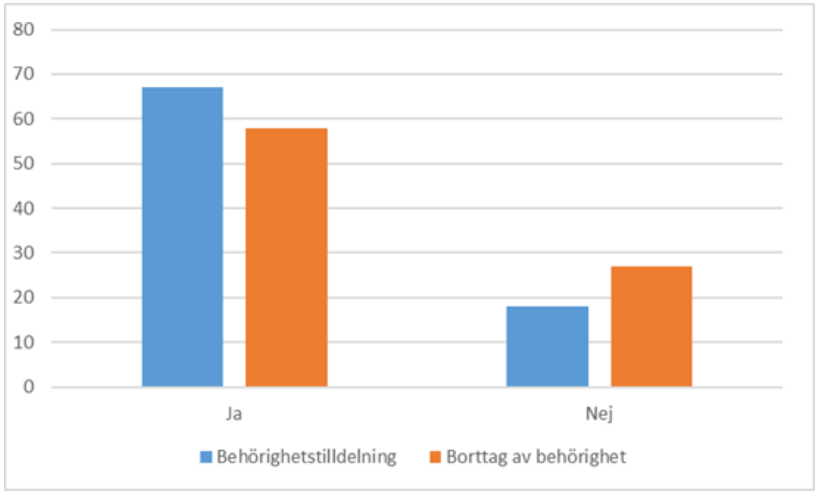

Är medarbetarna informerade om vad en personuppgiftsincident och IT-incident är och hur det ska anmälas?



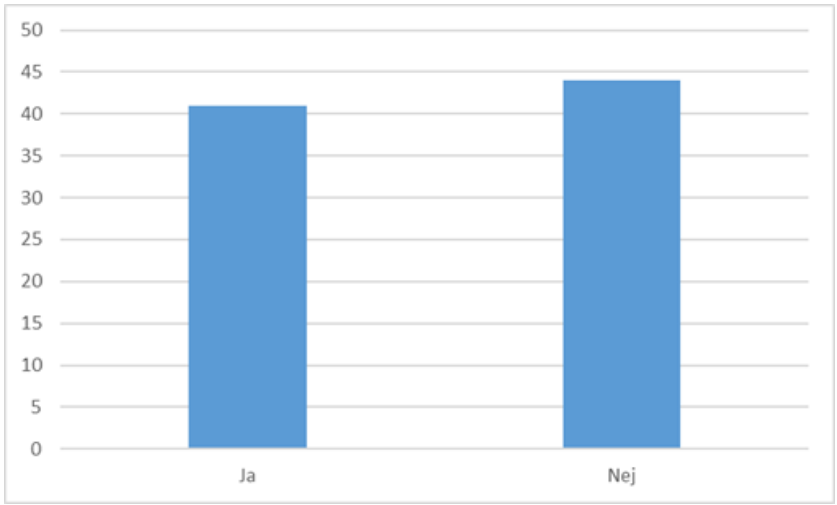

Har medarbetarna informerats om




Har ni i er verksamhet tydliga rutiner för behörighetstilldelning och borttag av behörighet för de IT-stöd som ni använder?




Finns det stöd som behövs i regionen för att arbeta  med informationssäkerhet?



### 5.3.1 Sammanställning av synpunkter från verksamheten om avsaknad av stöd

Efterfrågan av stöd kan delas in i fem punkter, behörighetshantering, molntjänster, information/utbildning, stödfunktioner samt information på intranätet. Följande har rapporterats in:

**Behörighetshantering**
Verksamheten upplever att det är svårt att veta vilka IT-stöd en person har behörighet till när en person har arbetat en längre tid i regionen. En önskan finns att det för varje IT-stöd finns en årlig uppföljning av behörigheter så en rensning av behörigheter kan ske när en person har bytt arbetsuppgifter.

**Molntjänster**
Verksamheten upplever mycket osäkerhet kring exempelvis molntjänster samt vid outsourcing generellt hantering av PUB-avtal.

**Information och utbildning**
Generellt så behövs en kunskapsuppbyggnad och repetitionsutbildningar i frågor kopplade till informationssäkerhet. Det upplevs en viss otydlighet om vad som gäller och det finns ett behov av utbildning och information för flertalet medarbetare och chefer.

Detaljer kring informationssäkerhetsarbetet inklusive GDPR och juridik kan inte hanteras i verksamhet annat än om vi skulle anställa en person för detta, en central funktion som hjälper till med frågorna.

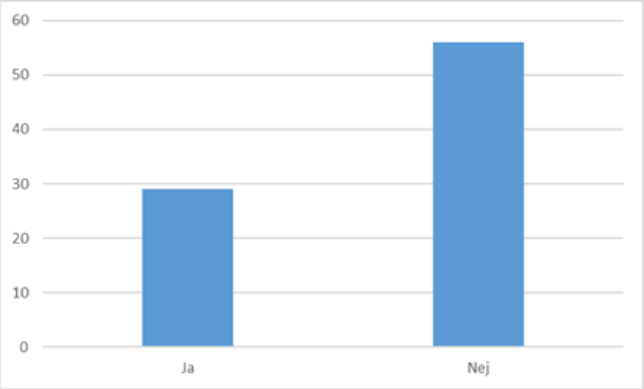
**Stödfunktioner**
Det behöver finnas centralt stöd även för det operativa genomförandet. Det är svårt att få till informationsklassning och riskanalys. Riktlinjer och rutiner är svåröversiktliga och medför alldeles för mycket tidsåtgång till att läsa sig in på hur man gör. Roller såsom Informationssäkerhetssamordnare som stöd vid ex. informationsklassning saknas. Allt finns beskrivet i rutiner och riktlinjer men det finns ingen fungerande organisation kring detta. Övergripande stöd saknas som kan ge ett stöd i den utsträckning som behövs på regionnivå och till förvaltningsnivå. En fungerande it-enhet med nödvändiga resurser samt en person som kan ge kortare information om sekretess och informationssäkerhet. It- stöd för att verksamheten ska kunna göra registeranmälan samt uppföljning av befintliga registeranmälningar.

**Information på intranätet**
Det generella intrycket är att medarbetare upplever det svårt att hitta rätt information på intranätet. Dokument finns men det är svårt att hitta informationen i dokumenten. En enklare information i dokumenten är att önska så det passar alla medarbetare. Det

behöver bli lättare att hitta vem som kan ge stöd och hjälp. Tillgängliga presentationer skulle underlätta i arbetet för att informera om informationssäkerhet till medarbetare.

### 5.3.2 Sammanställning av de prioriterade aktiviteter i verksamheterna som rapporterats in via enkäten

Frågan var: Har ni inom ert verksamhetsområde prioriterade aktiviteter inför 2022 inom informationssäkerhetsområdet?




**Följande rapporterades in:**

**Förbättringsåtgärder kopplat till IT-lösningar**

- Upphandling av nytt Tandvårdssystem.
- Införa Säkra meddelanden för att på ett säkert sätt dela och ta del av journalinformation mellan privat tandvård och patienter inom folktandvården.
- Arbeta igenom ett antal IT-system som körs via molntjänster och säkerställa att personuppgifter hanteras på korrekt sätt i hela flödet.

**IT-säkerhet**

- Införande av MFA för alla system i verksamheten. Säkra upp vissa funktioner och begränsa vilka som har access. (MFA multifaktorautentisering).
- Uppgradering av infrastruktur-versionshantering av databaser.

**Utbildning och information**

- Se till att all personal är uppdaterad på sitt ansvar inom informationssäkerhet
- Utbildning i informationssäkerhet för nya medarbetare.
- Utbildning runt GDPR Alla ska genomföra informations- och säkerhetsutbildning.
- Genomgång med verksamhetschefer om deras roll i informationssäkerhetsarbetet.
- Dataintrång tas upp årligen och extra om det sker avvikelser.

# 6. Förbättringsåtgärder

## 6.1 KLASSA

Regionen har idag verktyget ISAK för informationsklassning. Isak är en äldre Excelfil som är framtagen tillsammans med Region Dalarna. Verktyget/Excelfilen innehåller en mall för informationsklassning och riskanalys samt kravställning utifrån de tre säkerhetsaspekterna. ISAK är framtagen för att utföra informationsklassning riktat till IT-stöd. För att bedriva ett systematiskt informationssäkerhetsarbete ska all information klassas oavsett var i verksamheten den finns. Det kan exempelvis handla om system, processer eller arbetsflöden där olika informationsmängder hanteras. Detta arbete försvåras idag eftersom ISAK primärt är lämpat för informationsklassning av it-stöd.

SKR har under 2021 tagit fram ett webbaserat verktyg för informationsklassning och riskanalys, KLASSA, för att stödja kommuner och regioner i informationssäkerhetsarbetet med möjlighet att genomföra en informationsklassning och riskanalys kopplat till it-stöd, enskilda dokument och processer. Regionens informationssäkerhetssamordnare har varit delaktig arbetet tillsammans med SKR och andra regioner och har därmed haft möjlighet att påverka hur klassningsverktyget på ett lämpligt sätt ska kunna stötta verksamheterna i sitt arbete med informationsklassning och riskanalyser.

KLASSA bygger på modellen för informationsklassning enligt MSB:s metodstöd för systematiskt informationssäkerhetsarbete utifrån standard (SS-ISO/IEC 27001:2017) för ledningssystem och innehåller fyra delar: informationsklassning, kravställning/handlingsplan, upphandlingskrav och riskanalys.

KLASSA innehåller utbildningsmaterial och stödjande texter för informationsklassning och riskanalys som tillses av SKR, vilket underlättar genomförande av informationsklassning och riskanalys.

KLASSA är ett verktyg som är lämpligt för informationsklassning för all information, inte bara it-stöd. Verktyget kommer att ge regionen och informationsägaren en överblick av aktuella informationsmängder, pågående och genomförda informationsklassningar, handlingsplaner och tillhörande riskanalyser på en samlad plats. Verktyget kommer också att möjliggöra uppföljning av tidigare gjorda klassningar och riskanalyser. Vid förändringar som berör kravställning för informationshantering sker en uppdatering via SKR:s förvaltningsorganisation.

Regionens informationssäkerhetssamordnare fortsätter att bevaka och delta i arbetet med KLASSA. I detta arbete ingår också att undersöka möjligheten för regionen att i framtiden kunna använda sig av verktyget.

## 6.2 Utbildningsinsatser

De utbildningar som ges regelbundet har delvis genomförts digitalt. Exempelvis utbildning för chefer inom ramen för Formellt ledarskap, utbildning för ST-läkare, utbildning för studerande vid läkarprogrammet termin 8 ”Juridik, informations- och patientsäkerhet”.

Informationsinsatser har skett främst i digital form gällande roller och ansvar kopplat till informationssäkerhetsarbetet till ett fåtal ledningsgrupper. Vidare har informationsinsatser om hur informationsklassningar och riskanalyser ska ske ägt rum, även dessa till ett fåtal grupper i regionen.

Det finns en rekommendation att samtliga anställda ska genomföra den e-learningutbildning om informationssäkerhet (DISA) som finns att tillgå i regionens utbildningsportal PingPong. DISA är en utbildning som MSB har tagit fram som tar upp olika aspekter av informationssäkerhet. Utbildningen består av kortare filmer samt påståenden med efterföljande frågor. Utbildningen tar bland annat upp; säkert beteende, lösenord, e-post, skadlig kod, sociala medier, mobila enheter, molntjänster, säkerhetskopiering och loggning och spårbarhet.

# 7. Incidenter/avvikelser

Incidenter och avvikelser sker ofta genom systemfel och misstag. System och infrastrukturen är i dag både stora och komplexa samtidigt som de yttre hoten ökar i takt med digitaliseringen i dagens samhälle. Ett systematiskt informationssäkerhetsarbete är ett stöd vid kravställning av säkerhet och administrativa rutiner. Verksamheterna behöver därför prioritera informationssäkerhetsarbetet genom att tillsätta tid för kartläggning av processer och identifiering av informationstillgångar, identifiera informationsägare, genomföra informationsklassningar med tillhörande riskanalys och när krav ställs genomföra konsekvensbedömning.

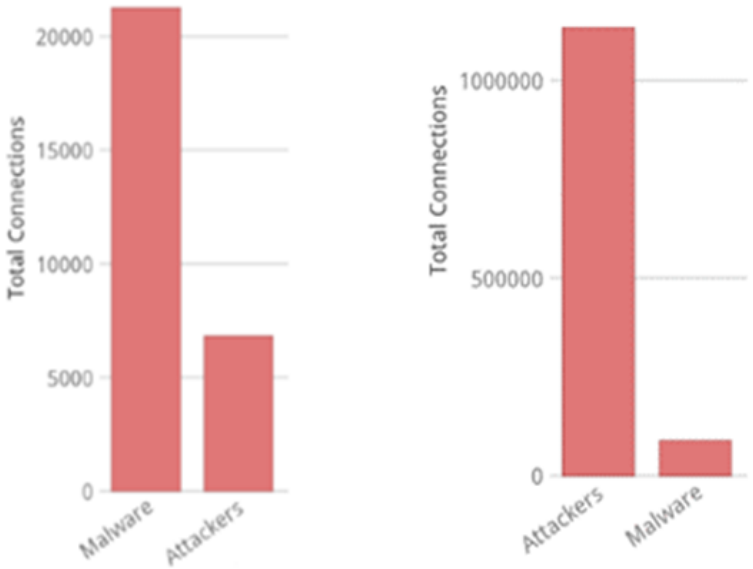
## 7.1 IT incidenter, ransomware och phising mm

### 7.1.1 Granskade och stoppade intrång via internet

Regionens intrångsskydd (IPS = Intrusion Prevention System) arbetar utifrån två huvudprinciper, det stoppar trafik utifrån avsändar-/destinationsadress och det analyserar dessutom övrig trafik efter ”signaturer” (dvs kännetecken) som tyder på skadligt beteende. Regionen har ett abonnemang och får fortlöpande information om svartlistade adresser och intrångs-signaturer som är förknippade med IT-brottslighet och skadlig mjukvara.

Undersöks den första sortens trafik (från/till svartlistade adresser) noteras att den aktiviteten gick upp kraftigt i början av Covid-perioden för att sedan gå ned på en lägre nivå. Nivån var fortsatt låg i början på 2021 men gick sedan upp kraftigt igen senare halvan av 2021.

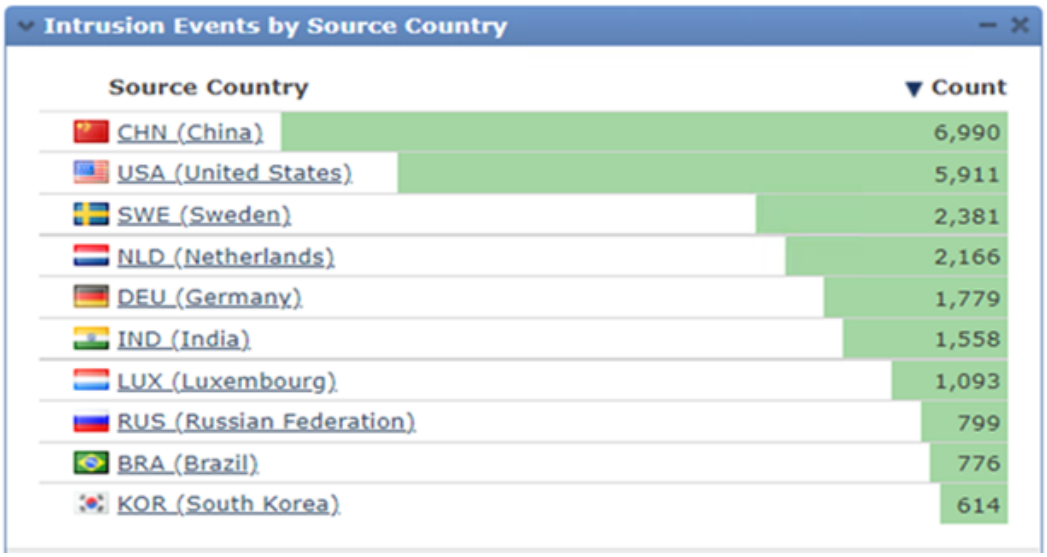
Diagrammen nedan visar exempel från två dygn under 2021 det vänstra från januari och det högra från december. Notera att skalan är olika. Exemplet från januari hade ca 7000 så kallade attackers och ca 21.000 malware. Motsvarande siffror i exemplet från december är ca 1.100.000 attackers och ca 100.000 malware.




Det är en mycket tydligt ökad aktivitet. Det mesta av denna trafik genereras säkerligen av automatiska genomsökningar efter sårbarheter men en del är också manuellt initierade attackförsök. Denna sorts bakgrundsbrus pågår hela tiden utan avbrott och blockeras direkt av regionens intrångsskydd. ”1.100.000 attackers” betyder inte att över en miljon olika hackers har försökt attackera regionen utan att ett antal ihärdiga förövare har försökt många tusentals gånger var.

Den andra sortens trafik (som matchar signaturer och kan tyda på mer riktade attacker) har varit mera konstant över tid men den gick också upp mot slutet på 2021. I detta fall så var det dock framför allt den s k Log4J-sårbarheten som stod för uppgången. Denna mycket allvarliga sårbarhet hanterades, med mycket möda, kring årsskiftet 2021/2022. I stort sett alla företag och organisationer med koppling till internet behövde skyndsamt täppa ingen det här hålet i säkerheten. IT-brottslingar var tyvärr snabba med att utnyttja sårbarheten vilket syntes i statistiken i form av ett ökat antal intrångsförsök.

Följande diagram visar vilket land intrångsförsöken kom ifrån under 2021, men de flesta typer av it-attacker kan dirigeras om via adresser i annat land så det är svårt att veta hur många av försöken som verkligen härstammar från varje land. Att Kina är överst i listan stämmer dock överens med erfarenheten från olika större studier av volymen offensiva it-aktiviteter per land.




### 7.1.2 E-post filter

E-postfiltret som regionen använder är en extern tjänst. Fram till början av november användes tjänsten Hosted Email Security från Trend men den har under november 2021 succesivt bytts ut till tjänsten Exchange Online Protection från Microsoft som även den hanterar mailflödet utanför regionens datahallar.

Det nuvarande mailfiltret har också funktionen att sätta inkommande misstänkta mail i karantän där mottagaren, och administratörer, kan granska mailen utanför regionens egen miljö för att kunna släppa in mail som bedöms vara ok. Baserat på det kan filtret ”lära sig” hur inkommande mail bör klassificeras.

Merparten av de blockerade mailen klassar tjänsterna som "Spam" eller "Skräppost". I de fall ett mail innehåller en av tjänsten ej provad och godkänd länk så skrivs länken om så att man först landar hos den externa tjänsten som undersöker målsiten, vilket minskar risken avsevärt för att klicka på en skadlig länk.

Mail från mailservrar på ökända IP-adresser blockeras och listorna på adresser underhålls löpande.

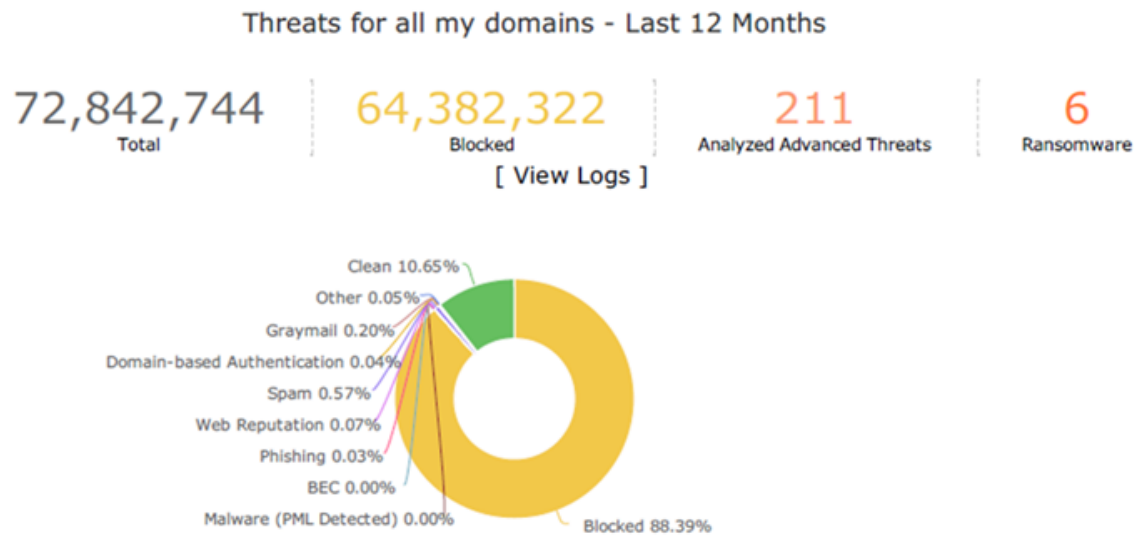
I och med det succesiva leverantörsbytet så är det svårt att få fram någon bra sammanhängande statistik eller trend baserat på kalenderår samt att rapporterna skiljer sig en del åt mellan tjänsterna.

Totalt under löpåret 2020-11-01 - 2021-11-01 har det till alla regionens domäner adresserats 72 842 744 mail. Av totalen har 64 382 322 mail blockerats, mestadels av de algoritmer som tjänsten sätter och hanterar men också av regler regionen kan påverka.

Av de drygt 52 miljoner blockerade mailen framgår att 128 identifierades som Advanced Threats och 52 identifierades som Ransomware.

Bara 10,65% av alla mail adresserade till regionen släpptes igenom till våra lokala mailservrar. Ur information från mailfiltren kan vi bara se vad som av en eller annan anledning har stoppats och i viss mån varför, inte vilket innehåll som har släppts igenom.

Nedan visas statistik från det gamla filtret Hosted Email Security från Trend



## 7.2 Världomfattande IT-attacker

I december 2021 upptäcktes en global och mycket allvarlig sårbarhet i en it-komponent som är vanligt förekommande i it- system och it- tjänster världen över (log4j). Ett meddelande skickades från Cert.se en funktion som tillhandahålls av MSB.

Sårbarheten, som innebär att en hotaktör på ett enkelt sätt kan ta sig in i it- system och antingen stjäla information eller installera skadlig kod (virus med mera) i it- miljön, hade den högsta klassningen på en 10-gradig skala.

Regionservice IT startade ett intensivt arbete med kontroller och säkerhetshöjande åtgärder i samarbete med andra regioner. Zip-filer stoppades i e-postfiltret då det var den största sannolikheten att den skadliga koden skickades vi mail i bifogade Zip-filer. Ett meddelande skickades ut till alla medarbetare via intranät med uppmaning att vara uppmärksamma på inkommande mail.

## 7.3 Driftavbrott i Vårdsystem

Under 2021 har regionen haft fem incidenter i våra journalsystem Infomedix och NCS Cross. Incidenterna har påverkat en större del av användarna.

## 7.4 Personuppgiftsincidenter

Under 2021 har det registrerats 202 misstänka personuppgiftsincidenter i Platina, av dessa är det två som anmälts vidare till Integritetsskyddsmyndigheten, IMY. Det som är återkommande är kallelse/brev skickas till fel patient.

# 8. Fokusområden 2022

## 8.1 Det systematiska informationssäkerhetsarbetet

Regionen behöver förbättra informationssäkerhetskulturen. Kunskapen och medvetenheten behöver öka om de krav som ställs vid behandling av information i alla former. Informationssäkerhetsarbetet kan då bli mer effektivt och systematiskt.

En viktig del är att få Ledningssystem för informationssäkerhet (LIS) på plats. Ett grundläggande förslag finns framtaget och presenterat för informationssäkerhetsrådet. Ledningssystemet ska vara vägledande i de olika faserna i det systematiska informationssäkerhetsarbetet samt innehålla de ”verktyg” som behövs för att bedriva

arbetet. De styrande dokumenten ses löpande över för att uppdateras och utgör bas för innehållet i ledningssystemet.

Det är en utmaning är att öka kunskapen och bygga upp en kompetens kring informationsklassningar och riskanalyser. I takt med den snabba digitalisering som nu sker märks också att denna kompetens ofta efterfrågas.

Uppföljning av informationsklassningar med tillhörande riskanalys behöver även förbättras. Enligt de fritextsvar som är inskickade via enkäten så finns det en generell avsaknad av stöd i verksamheterna i det systematiska arbetet. Det pågår ett arbete med ett diskussionsunderlag i syfte att förbättra detta stöd.

Informationsklassningar och riskanalyser kommer alltid att behöva ske i verksamheter som hanterar information. Det ingår i det systematiska informationssäkerhetsarbetet och dataskyddsarbetet som ska finnas inom alla regioner och kommuner. Således är det här ett ständigt återkommande arbete för regionen liksom för alla andra organisationer som hanterar information.

## 8.2 NIS-direktivet och NIS-lagstiftningen

Den 6 juli 2016 antogs NIS direktivet av Europaparlamentet. Direktivet har implementerats i den svenska lagstiftningen genom en svensk NIS lag och NIS förordning. Dessa trädde i kraft under 2018. I slutet av 2018 publicerade MSB föreskrifter till NIS lagstiftningen. De nya reglerna omfattar leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster. Regionen omfattas utifrån området hälso- och sjukvård inklusive tandvård.

Reglerna ställer bland annat krav gällande säkerhetsåtgärder, incidentrapportering och tillsyn. Regelverket ställer krav på att de verksamheter som omfattas ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Här handlar det om att identifiera de system som kan vara kritiska för att den samhällsviktiga tjänsten, hälso- och sjukvård ink. tandvård ska kunna bedrivas.

Lagstiftningen innebär bland annat:

- Krav på leverantörer av samhällsviktiga tjänster att arbeta systematiskt och riskbaserat med informationssäkerhet.
- Krav på leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster att rapportera incidenter till utpekad myndighet.
- Att ett antal myndigheter får i uppgift att bedriva tillsyn inom sina respektive sektorer.

Utifrån NIS-lagstiftningen har således hälso- och sjukvården och tandvården ett särskilt krav på sig att bedriva ett systematiskt informationssäkerhetsarbete. Däri ingå att kartlägga vilka system/tjänster/infrastruktur etc. som är av särskild vikt för att vårdgivaren ska kunna leverera den samhällsviktiga tjänsten hälso- och sjukvård och tandvård. I lagen finns också ett krav att rapportera s k NIS-incidenter. Till exempel kan en incidentanmälan till MSB behöva ske om ett vårdsystem ligger nere under en längre tid och vården påverkas.

För att kunna leva upp till kraven i NIS-lagstiftningen behöver hälso- och sjukvården och tandvården beskriva vilka krav som ställs på respektive vårdsystem för att kunna upprätthålla det samhällsviktiga uppdraget. Detta arbete behöver ske tillsammans med Regionservice IT. Det här arbetet behöver prioriteras.

## 8.3 FVIS (Framtidens vårdinformationssystem)

Under 2020 och delar av 2021 ingick jurist och/eller informationssäkerhetssamordnare i en referensgrupp för informationssäkerhet och juridik. Syftet med gruppen är att delta i FVIS-arbetet med att ta fram förutsättningar för införande av regionens och SUSSA-regionernas nya vårdinformationssystem. Detta arbeta stannade dock av under större delen av 2021. Behovet av stöd i informationssäkerhet- och juridikfrågor i VISUS-arbetet kvarstår dock.