

Security of Information and Innovation

May 2021





Security of information

1. Risks related to information systems



The main risks related to information systems for Ferreycorp are:

Interruption of business operations

Events associated with the Interruption of business operations due to IT and environmental threats:

- Prime & Rentals
- Spare parts
- Workshop and Field Services
- Specialized Workshop Services
- Logistics
- Industrial Fuels
- Accounting
- Financial services
- Human Resources

Fraudulent operations

Events associated with illegal activities or dishonest practices that harm the Corporation's companies. Includes: deception, counterfeiting, fraud, etc

- Appropriation of money
- Inventory appropriation
- Payments to suppliers
- Employee payments
- Client payments

Leak or loss of sensitive information

Eventos asociados a la salida no controlada de información hacia personas y/o empresas no autorizadas.

- Información Estratégica
- Información de Productos y Servicios
- Información sobre Cotizaciones
- Información Técnica
- Información Financiera
- Información de Comercial
- Información de Recursos Humanos

Legal, Regulatory and Reputational Compliance

Events associated with contractual breach with partners, legal requirements and negative exposure of the Corporation's brands.

- Fines and penalties.
- Damage to image and reputation

2. Scope of the Information Security Management System



Dealer Intelligence Network (DIN)

We are part of the DIN, whose purpose is to share cyber threats of interest to Caterpillar and its dealers. The objectives of the DIN are:

- Reduce the impact of threats and proactively protect our organizations
- Share data and intelligence, which allows us to implement security controls.
- Reveal common trends, patterns, and threats.

News about Cybersecurity

CYBER THREAT INTELLIGENCE FOR MARCH 9, 2021

Threat Actor Spotlight: China hacks at least 30,000 U.S. organizations via **Microsoft Exchange Server** vulnerabilities.

A Chinese state-sponsored group referred to as **Hafnium** conducted targeted attacks on email systems used by multiple industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs.



Threat Spotlight: China-linked hackers exploited SolarWinds software in 2020 breach.

Threat Spotlight: Fake Google reCAPTCHA phishing attack steals Office 365 passwords.



Best Practices

| Threads |
|----------------------------------|
| Thread |
| DFARS Cyber Security Compliance |
| Microsoft LAPS |
| DMARC Implementation |
| Information Classification |
| CDN Discussions instead of Email |

Threats and vulnerabilities

| Threads |
|--|
| Thread |
| 2021-03-12-Daily Observed Dealer Fuzzy Domains |
| 2021-03-12-Daily Observed Domains |
| 2021-03-11-Daily Observed Dealer Fuzzy Domains |
| 2021-03-11-Daily Observed Domains |

DIN Meet

Strategic, Operational, Tactical Briefs

Cybersecurity researchers targeted by North Korea.
In late January, Researchers at Google's Threat Analysis Group (TAG) published their findings into a campaign seen targeting Security Researchers.

The campaign used social engineering techniques to lure security researchers to collaborate on vulnerability research, but ultimately delivered malware disguised as a Microsoft Visual Studio Project. Threat actors maintained a blog site that was promoted by various twitter accounts that were owned and controlled by the threat actors.

The blog contained vulnerability and exploitation research from previously disclosed cve's. The blog site also doubled as a "watering hole", delivering malware to visitors of the site. Researchers claim that the delivery method of the malware used a Chrome Zero-Day Vulnerability that was topic of the blog cover in October of 2020.

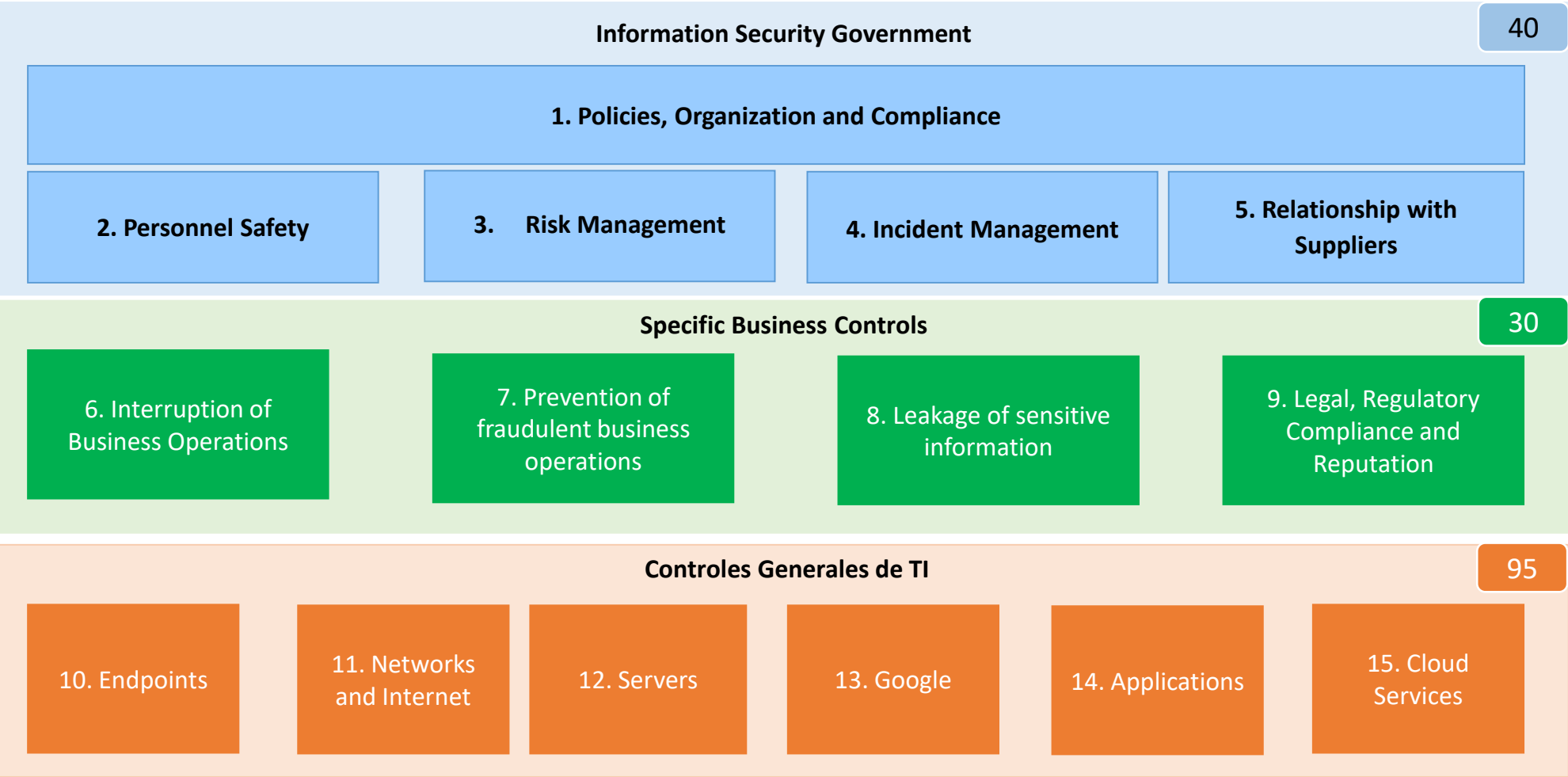
Water treatment facility hacked: OT (ICS, SCADA, IoT) Network Threats
On February 5, 2021, unidentified cyber actors obtained unauthorized access to the supervisory control and data acquisition (SCADA) system at a U.S. drinking water treatment facility and attempted to elevate levels of sodium hydroxide by a factor of more than 100.

Elevated levels can cause physical harm to the public.

The remote attacker reportedly exploited cybersecurity weaknesses, including poor password security, and an outdated operating system (windows 7) and possibly used TeamViewer, a remote access tool.

Hackers could cause serious damage to organizations by targeting exposed human-machine interfaces (HMIs), and the incident in Oldsmar is another reminder of how vulnerable such systems across the nation's critical infrastructure can be.

3. Information Security Management Model



Total N° of controls

165

N° of controls related to cybersecurity

67

4. Current Situation

Self-evaluation



At the end of February 2021, a self-evaluation was carried out to measure and analyze the impact of the following topics:

| | |
|--|---|
| Information Security Government | |
| Policies, Organization and Compliance | |
| Personnel Safety | |
| Risk Management | |
| Incident Management | 1 |
| Relationship with Suppliers | |
| Specific Business Controls | |
| Business Operations Interruption | 2 |
| Fraudulent Operations Prevention | |
| Information Loss / Leak Prevention | |
| Legal and Regulatory Compliance | |
| General IT Controls | |
| Endpoints | |
| Servers | |
| Connectivity | 1 |
| Google | |
| Applications | 1 |
| Cloud Services | |

- 1 Strengthen network security monitoring and cloud services and integrate it into incident management
- 2 After the departure from SAP Hana, it is required to develop and test a DRP for SAP and complementary systems.

5. Roadmap

2017 - 2020



| |
|---|
| Information Security Government |
| Information Security Government |
| Security Policies |
| Compliance revisions |
| Personnel Safety |
| Staff Awareness |
| Risk Management |
| Vulnerability Analysis - Ethical Hacking |
| Vulnerability Analysis - Web Applications |
| Incident Management |
| Incident management process |
| Relationship with suppliers |
| Security in integration with suppliers |
| Specific Business Controls |
| Business Operations Interruption |
| DRP (DBS, SAP R3) |
| Fraudulent Operations |
| Segregation of duties - HR |
| Segregation of Duties - Purchasing (SAP Hana) |
| Segregation of Duties - Sales (SAP Hana) |
| Segregation of Duties - Treasury (SAP Hana) |
| Information leakage |
| Information Leak Prevention |
| Rules preventing impersonations |
| Double Factor Authentication |
| Legal and regulatory compliance |
| Compliance with the Data Protection Law |
| Compliance Authorized Economic Operator |
| BASC Operator Compliance |

| |
|--|
| General IT Controls |
| Endpoints |
| Antimalware endpoints and servers |
| Endpoint intrusion prevention |
| Secure configuration for endpoints |
| Servers |
| Secure configuration for servers |
| Vulnerability and patch management |
| Privileged access on servers |
| Conectivity |
| Firewall, IPS |
| Wireless Security |
| Routers and switch security updates |
| Google |
| Antimalware, Antispam , 2FA |
| Monitoring of improper access |
| Google Drive Security |
| Applications |
| Periodic access reviews |
| Block unused accounts / terminated staff |
| Access controls in business applications |
| Encryption of sensitive data - Central Covid |
| Cloud Services |

5. Roadmap

Plan for 2021



Information Security Government

Policies, Organization and Compliance

- Security Policies - Policy update
- Independent reviews (Marsh, Internal Audit)

Personnel Safety

- Staff Awareness - Material Update
- Disciplinary process with HR for breach of policies

Risk Management

- Vulnerability Analysis - Ethical Hacking
- Vulnerability Analysis - Web Applications

Incident Management

- Integrate Incident Management with Security Monitoring
- Define security alert thresholds
- Define specific management procedures (Ransomware, Attacks)

Relationship with suppliers

- Validate security controls integration with supplier networks

Specific Business Controls

Business Operations Interruption

- Disaster Recovery Plan - SAP Hana and Satellites

Fraudulent Operations

- Compliance monitoring of Segregation of Duties Rules

Information leakage

- Information Leak Prevention - (Google and USB)

Legal and regulatory compliance

- Compliance with the Data Protection Law

General IT Controls

Endpoints

- Antimalware on cell phones
- Evaluation of software installed on endpoints

Servers

- Restriction of privileged access to servers and IT services

Google

- Security configuration review

Applications

- Restrict access in business applications
- Fix web application vulnerabilities
- Make adjustments to the Model Roles

Conectivity

- Network Security Monitoring

Cloud Services

- Cloud security monitoring



Ferreycorp

Innovation

Innovation

Culture and Develop of Capabilities

Leadership

Developing mindset leaders in customer-centric digital transformation

- Developing Program “Por los próximos 100 años”
- Planning “Cumbre de Innovación 2021”
- Performance Management in Innovation Projects
- 54 Priority Innovation and Transformation Initiatives

Talent

Aligning the leadership of middle management in customer-centric digital transformation.

- Innovation Tools (Toolkit) and workshops
- Innovation chanel: Portal de Innovación

Program “Por los próximos 100 años”*

Results



November 2020 – May 2021

510 leaders

21 sessions

- Cross to the Corp : **2**
- Digital Age skills: **6**
- Leadership skills: **7**
- Business Talks: **6**

May – Jul 2020

227 leaders

23 sessions

- Current environment: **3**
- Lead in Uncertain Times: **4**
- Business: **12**
- New ways of work: **4**

Satisfaction Survey Results (average)

4.5/5
Quality
content

4.5/5
Quality
speakers

4.6/5
Useful
Therms

* “For the next 100 years”



On the image:
Some participants of
the “Por los próximos
100 años” Program
explained above,
ranging from
managers and key
personnel to invited
speakers

Program “Por los próximos 100 años” Results



To the date

82 workshops
~1300 participants

Developing of
capabilities

10 Innovation
Agentes
Sessions
~275 participants

Open Innovation
circles & Tour
Companies
~187 participants



Innovation

Customer Centric Prioritized Initiatives

Digital Customer Experience

Facilitate the interaction between customers and Ferreycorp companies

- Centralized customer data Management.
- Digital customer self service portal for logistic services.
- Spare order tracking.

E-Commerce

Increase sales in certain lines and facilitating the shopping experience for our customers

- E-Commerce for spare parts.
- Direct purchase of spare parts through the integration of ERP.
- E-commerce platforms for subsidiaries.

Supply Chain

Delivering Products and services to customers at the required time and at the lowest possible cost

- Order traceability from purchase order to customer delivery.
- Shared services for corporate cargo.
- Optimization of warehouse management processes.

Innovation

Customer Centric Prioritized Initiatives

Productivity

Optimize equipment productivity by taking advantage of digital solutions

- Maximize equipment/machinery connectivity
- Remote assistance and site monitoring to increase the availability and reliability of equipment

New products and digital services

To satisfy the needs of our clients through new product and services based on digitalization

- Customer centric marketplaces (Operators, Used equipment, Education)
- Quipu: Spare parts microcredits for small contractors.
- Autonomous trucks in mining pits
- Mining productivity solution platform based on multibrands equipment connectivity and information management.

Innovation

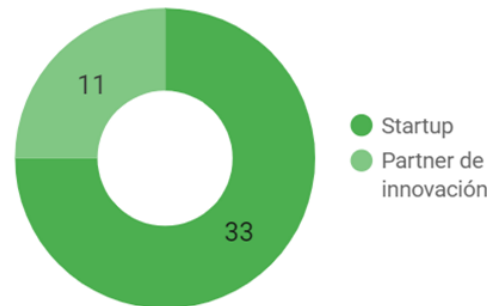
Open Innovation



Open Innovation Repository

During 2020 we had explored partnerships with 44 enterprises, 11 of them were startups and the remaining 33 were companies. We are currently collaborating with 6 of them in Innovation projects.

We use a Dashboard to follow up the initiatives and for knowledge management purpose.



Directorio de Innovación Abierta

Nº Entidades contactadas
44

| Tipo | Nº |
|--------------------------|----|
| 1. Startup | 33 |
| 2. Partner de innovación | 11 |

| Giro | Nº |
|----------------------|----|
| Fintech | 8 |
| Geoespacial | 1 |
| Gestión de Flota | 3 |
| Gestión de activos | 1 |
| Gestión de proyectos | 1 |
| Industria 4.0 | 1 |

| Organización | Tipo | Giro | Representante | Iniciativa |
|----------------------|-----------------------|-----------------------------------|-----------------|--|
| 1. Activate Machines | Startup | Gestión de Flota | Brian Giamo | Plataforma de gestión de equipos multimarca para clientes retail |
| 2. Ambidextro | Partner de innovación | Diseño de experiencia de usuarios | Iván Juscamaíta | Partner de innovación para proyectos estratégicos |
| 3. AmigoCloud | Startup | Geoespacial | Ragi Burhum | Gestión geoespacial y de ubicación |